# 量子コンピュータと量子通信 II

## 量子コンピュータとアルゴリズム

Michael A. Nielsen, Isaac L. Chuang 共著／木村達也 訳

Quantum Computation and Quantum Information

Ohmsha

両親と恩師に捧げる

# まえがき

本書は量子計算と量子情報分野における主要な概念と技術に対する入門の役割を果たすものである．急速な進展と分野横断的な性格のために入門者がこの分野の最も重要な技術や成果を広く知ることが難しいのが現状である．

本書の目的は 2 つある．第 1 は量子計算と量子情報を理解するに必要なコンピュータ科学，数学及び物理学の基礎知識を提供することである．これら 3 分野の 1 つまたはそれ以上の分野における，学部学生と少なくとも同レベルの素養と，量子計算と量子情報を学ぶ希望を持つ読者を対象としている．本書の第 2 の目的は量子計算と量子情報に関する中心的成果を詳細に提供することである．全体を読み通すと読者は一般的教養として，あるいは量子計算と量子情報の研究への入門として，この刺激的分野における基本ツールと，その成果に対する実効ある理解力を身につけることができる．

## 本書の構成

本書の基本構成を図 1 に示す．本書は 3 部より成る．全体の基本姿勢として具体的なものから始めて抽象的内容に進むことを可能な限り心がけた．したがって，本書全体を通じて一般的理論を展開する前に実例を提示することとし，量子情報より先に量子計算を，一般的量子情報理論より先に具体的量子誤り訂正符号を扱うこととしている．

第 I 部では量子計算と量子情報分野における主要概念と成果を広く概観し，同分野を深く理解するに必要なコンピュータ科学，数学，物理学の基礎知識を学ぶ．1 章はこの分野の歴史的発展と基本概念を概観する入門的な章であり，その中で幾つか重要な疑問点を浮き彫りにする．その内容はコンピュータ科学や物理学の知識背景なしに理解できる構成となっている．より詳細を理解するに必要な基礎

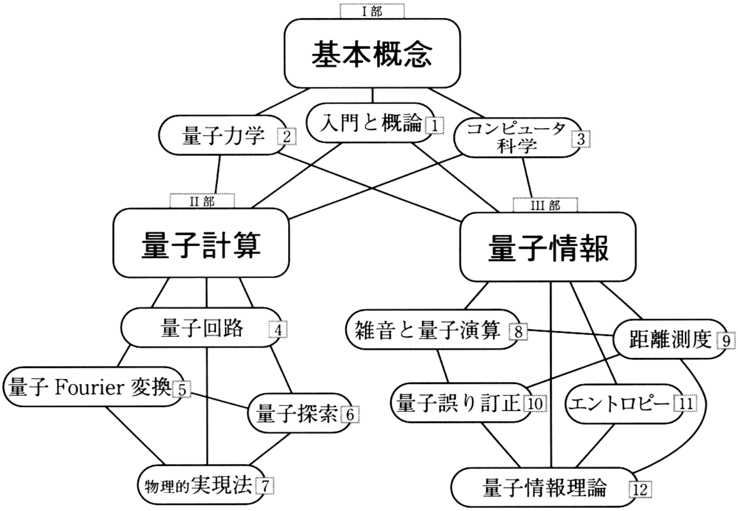



**図 1:** 本書の構成

知識は2章と3章で深められる．ここではそれぞれ量子力学とコンピュータ科学に関する基本概念を詳しく取り扱う．第I部の各章は読者の知識背景に応じて読み飛ばしても差し支えなく，量子力学やコンピュータ科学の基礎知識にギャップを感じたときに立ち戻ればよい．

第II部では量子計算について詳細に述べる．4章で量子計算を行うに必要な基本要素について述べ，複雑な量子計算の応用に使う多くの基本操作を示す．5章と6章は現在知られている2つの基本的量子アルゴリズムである量子 Fourier 変換と量子探索アルゴリズムについて述べる．5章ではまた量子 Fourier 変換を使った素因数分解や離散対数問題の解法と，それらを応用した暗号について説明する．7章では研究室で示された幾つかの実例を使って，量子コンピュータの一般的設計原理と望ましい物理的実現法の基準について述べる．

第III部は量子情報を取り扱う．量子情報とは何か，量子状態を使って如何に情報を表現し伝達するか，量子情報や古典情報の劣化を如何に表現しそれに対処するか等である．8章は実世界の量子情報処理を理解するのに必要な**量子雑音**の性質と，量子雑音を理解するための強力な数学ツールである **量子演算形式**について述べる．9章では2つの量子情報が似ているということが何を意味するかを，定量的に正確に表現できる量子情報の**距離測度**について述べる．10章では雑音の影響

から量子計算を守るのに使う，量子誤り訂正符号について説明する．この章で紹介する重要な結果は**しきい値定理**であり，これは現実的雑音モデルにおいて**原理上**雑音が量子計算の深刻な障害にならないことを示す．11 章では**エントロピー**の情報理論的基本概念を紹介し，古典情報理論と量子情報理論の両方におけるエントロピーの性質を説明する．最後に 12 章で量子状態と量子通信チャンネルがもつ情報を運ぶ性能を議論し，古典的および量子的情報伝送や秘密情報伝送に対する，奇妙な興味ある性質について詳しく述べる．

本書を通じて数多くの演習と問題が提供されている．演習は基本的内容を確実に理解することを目的として，本文の途中に示されている．二三の例外を除きこれらの演習は数分で容易に解くことができる．問題は各章末尾に配置されており，本文中で十分に述べる余裕がなかった新しい興味ある材料を，読者に紹介するためのものである．しばしば問題は複数部分に分かれており，特定の深い思考方向に導くように意図されている．少数であるが本書刊行時点で解が示されていない問題もあり，その場合には課題中にその旨が述べられている．各章末にその章の主要結果のまとめを示すと共に，その章全体に関する引用文献を通して主要概念の発展経緯を示し，次のステップの資料を示唆する「歴史と参考資料」の節が設けられている．

本書の冒頭に詳細な目次があるので一覧して頂きたい．また用語と記号の手引きを載せたのでこれも読者の役に立つであろう．

巻末に 6 つの付録と参考文献および索引を収録した．付録 A では確率論の初歩に関する基本的定義，記号および結果をまとめた．この内容は読者に既知と思われるが参照の便宜のために掲載してある．同様に付録 B に読者の便宜のために群論の基本概念をまとめておいた．付録 C では量子計算のための重要な成果である Solovay-Kitaev の定理の証明を示した．この定理は任意の量子ゲートが有限個の量子ゲートで近似できることを示すものである．付録 D は素因数分解や離散対数に対する量子アルゴリズムや，RSA 暗号システムを理解するに必要な整数論の基本をまとめた．RSA 暗号システムについては付録 E で解説する．付録 F では量子計算と量子情報における最も重要な結果の 1 つであり，有名な強い劣加法性不等式 (strong subadditivity equality) のような重要なエントロピー不等式の先駆でもある，Lieb の定理の証明を示す．Solovay-Kitaev の定理と Lieb の定理の証明は非常に長いので，本文と別に扱うことにしたものである．参考文献では

本文中に引用した全資料のリストを収録した．迂闊にもこの引用から洩らしてしまった業績の研究者にはお詫び申し上げる．

量子計算と量子情報の分野は近年急速に進歩したため，全トピックスを望み通りの詳しさで網羅することができなかった．3つの分野については特に述べておく必要がある．第1は**もつれの尺度**(entanglement measure) の話題である．本文で説明するようにもつれは量子テレポーテーション，高速量子アルゴリズム，量子誤り訂正等における重要な要素であり，手短に言えば量子計算と量子情報の優れたユーティリティ資源である．もつれの概念を新たな物理的資源として充実させ，その操作と有用性を左右する原理を見出している活発な研究グループが現在存在する．これらの研究は将来大いに有望ではあるが，本書で広範に記述した他の話題と同様な扱いをするにはまだ十分でないと我々は感じており，12章で簡単に触れるに止めた．同様に分散量子計算（量子通信コンプレックスとも呼ばれる）は活発に発展している非常に有望な課題なので，本書の出版時点でもすでに時代遅れになっていることをおそれて取り扱うのを控えた．量子情報処理デバイスの実現も肥沃で魅力ある分野に発展してきたが，この話題については1つの章を当てるに止めた．明らかに物理的実現に関してもっと多くを述べることができるが，それを始めると関連する物理学，化学，工学の多くの分野に言及せざるを得ず，十分なスペースを割くことができなかった．

## 本書の使い方

本書は幅広くいろいろな使い方が可能である．量子計算や量子情報の特定のトピックスに関するショートコースから，全分野を網羅する1年間の講義に至るいろいろなコースの材料として使える．量子計算や量子情報について少し勉強してみようという方や，研究の最前線にまで知識を高めたいという方が個人的に勉強するのに役立つ．また，この分野の現役研究者にも参考資料として役立ててもらうのが著者の希望である．我々はこの分野に参加する研究者の入門用として特に価値を認められることを望んでいる．

## 個人読者の方々へ

本書は個人読者に読みやすいように工夫している．本文を通じて多くの演習が用意され，本文内容の理解度を自分でチェックできる．目次と章末のまとめを使ってどの章を深く学ぶべきかを容易に決められる．図 1 の関連分野ダイヤグラムは本書の材料をどういう順序でカバーするかを決める際に役立つであろう．

## 教師の方々へ

本書は広範囲のトピックスを網羅しているので，いろいろな種類のコースの材料として使うことができる．

量子計算の半年コース用教材ならば，クラスの学力に応じて 1 章から 3 章までの内容を選択し，次に量子回路の 4 章，量子アルゴリズムの 5・6 章，および物理的実現の 7 章の中の幾つかを選び，さらに量子誤り訂正を理解するために 8～10 章，特に 10 章に焦点を絞るとよい．

量子情報の半年コース用教材ならば，クラスの学力に応じて 1 章から 3 章までの内容を選択し，次に 8～10 章の量子誤り訂正，11 章と 12 章の量子エントロピーと量子情報理論を選ぶとよい．

1 年間のコースならば本書の全章を当て，さらに数章の「歴史と参考資料」から資料を選んで時間を充当することができる．また，量子計算と量子情報は学生の個人的研究テーマとしても最適である．

量子計算と量子情報の講義以外にも本書を利用して頂きたいのは，物理学の学生のための量子力学入門の講義である．従来の量子力学入門は偏微分方程式の数学手法に過度に依存してきたきらいがある．我々はこれがしばしば基本概念を不明確にすると信じている．量子計算と量子情報は数学的手法にあまり依存することなく，量子力学の基本概念と比類ない特徴を理解する格好の優れた思考場所を提供する．そのような講義では 2 章の量子力学入門に焦点を絞り，4 章の量子回路に関する教材，5 章と 6 章の量子アルゴリズムの抜粋，7 章の量子計算の物理的実現，そして III 部から好みに応じた部分を付け加えるとよい．

## 学生の皆さんへ

本書はできるだけ自己完結的に書かれている．主な例外は自分自身で納得するための議論を所々で省略したことであり，これらは通常演習の形で与えられている．本書を通読するに当たって全演習を少なくとも試みてみることをお勧めする．少数の例外を除いて演習は数分で解くことができる．もし多くの演習に多大の困難を感じるならば，もう一度立ち返って１つあるいはそれ以上の重要な概念を復習し直す必要性を示唆しているかも知れない．

## さらに高度な資料

すでに述べたように各章末に「歴史と参考資料」の欄が設けてある．また読者が興味を持つかも知れない広範囲の参考資料も二三存在する．Preskill のすばらしい講義録 [Pre98b] は量子計算と量子情報に対して本書と少し異なる観点からアプローチしている．特定の主題に関する優れた解説論文を本書に現れる順に列挙すると，Aharonov の量子計算に関する解説 [Aha99b]，Kitaev の アルゴリズムと誤り訂正に関する解説 [Kit97b]，Mosca の量子アルゴリズムに関する学位論文 [Mos99]，Fuchs の量子情報の識別性と距離測度に関する学位論文 [Fuc96]，Gottesman の量子誤り訂正に関する学位論文 [Got97], Preskill の量子誤り訂正に関する解説 [Pre97], Nielsen の量子情報理論に関する学位論文 [Nie98], Bennett, , Shor [BS98], Bennett, DiVincenzo [BD00] による量子情報理論の解説がある．この他にも Gruska の著書 [Gru99]，Lo，Spiller，Popescu 編集になる解説論文集 [LSP99] が有用である．

## 正　誤

長大な文書にはしばしば誤りや欠落が伴う．本書もこの法則の例外ではない．もし，読者が誤謬を見つけたり，本書に関して異なるご意見をお持ちならば，qci@squint.org にメールを下さるようお願いする．見つかった誤りは本書の Web サイト http://www.squint.org/qci/ のリストに追加する．

# 謝　辞

量子計算と量子情報について我々は数人の方々から決定的な影響を受けた．我々の考えを形成し洗練するのに大いに役立った多くの楽しかった議論に対して，MAN は Carl Caves，Chris Fuchs，Gerard Milburn，John Preskill および Ben Schumacher に，ILC は Tom Cover，Umesh Vazirani，Yoshi Yamamoto および Bernie Yurke に感謝する．

本書の執筆には非常に多くの人々から直接間接にご援助を頂いた．その一部をあげると，Dorit Aharonov, Andris Ambainis, Nabil Amer, Howard Barnum, Dave Beckman, Harry Buhrman, Caltech Quantum Optics Foosballers, Andrew Childs, Fred Chong, Richard Cleve, John Conway, John Cortese, Michael DeShazo, Ronald de Wolf, David DiVincenzo, Steven van Enk, Henry Everitt, Ron Fagin, Mike Freedman, Michael Gagen, Neil Gershenfeld, Daniel Gottesman, Jim Harris, Alexander Holevo, Andrew Huibers, Julia Kempe, Alesha Kitaev, Manny Knill, Shing Kong, Raymond Laflamme, Andrew Landahl, Ron Legere, Dabbie Leung, Daniel Lider, Elliott Lieb, Theresa Lynn, Hideo Mabuchi, Yu Manin, Mike Mosca, Alex Pines, Sridhar Rajagopalan, Bill Risk, Beth Ruskai, Sara Schneider, Robert Schrader, Peter Shor, Sheri Stoll, Volker Strassen, Armin Uhlmann, Lieven Vandersypen, Anne Verhulst, Debby Wallach, Mike Westmoreland, Cave Wineland, Howard Wiseman, John Yard, Xinlan Zhou, および Wojtek Zurek である．

本書をアイディア段階から出版までお世話になった Cambridge 大学出版の皆さんに感謝する．思慮深く情熱的な編集者 Simon Capelin はこのプロジェクトを 3 年以上にわたって指導し，Margaret Patterson は時宜を得て徹底した原稿編集をしてくれた．特に感謝する．

本書を執筆したのは，MAN が California 工科大学で Tolman Prize Fellow, Los

Alamos 国立研究所で T-6 理論宇宙物理学グループ研究員，および New Mexico 大学先端研究センタ研究員として在任中，一方 ILC が IBM Almaden 研究センタ研究スタッフ，Stanford 大学電気工学科助教授，California 大学 Berkeley 校コンピュータ科学部客員研究員，Los Alamos 国立研究所 T-6 理論宇宙物理学グループ研究員，California 大学 Santa Barbara 校理論物理学研究所客員研究員として在任中であった．本書の最終校正を完成した Aspen 物理学センタでの暖かいもてなしに感謝する．

MAN と ILC は NMRQC 研究イニシアティブのもとでの DARPA のご支援，陸軍研究オフィス下での QUIC 研究所によるご支援に深く感謝する．また，米国科学財団，米国国家安全局，海軍研究オフィスおよび IBM の寛大なご支援に感謝する．

# 訳者まえがき

本書は近年注目を集めている量子コンピュータと量子通信全般にわたる基本原理を懇切に述べた定本ともいうべき書である．原著の推薦文にはこの分野の発展に大きな貢献をした Michael Freedman, Charles Bennett, Peter Shor という錚々たる研究者が名を連ねており，学部レベル以上の理解力を持つ読者に向けて自己完結的な書物を書くことに成功しているとの評を与えている．この分野はすでに非常に大きくなりすべてをカバーすることはもはや困難になっているが，著者らは話題をよく選択してそれをわかりやすく説明している．

その大きな特徴は著者のまえがきにあるように，単純から複雑へ，実例から一般へ，具体から抽象へという姿勢を徹底して保っていることであり，理論主体の書でありながら読みやすく説明されている．ちなみに本文中に「直観」という言葉が実に百回以上も使われている．これは単に論理による説得ではなく，読者の論理的理解と直観的納得の整合を重視する著者の説明姿勢を端的に現わしている．

著者の一人 Michael A. Nielsen はオーストラリアのクイーンズランド大学の教授であり，ニューメキシコ大学，ロス・アラモス国立研究所，カリフォルニア工科大学等で研究業績をあげている．またもう一人の Isaac L. Chuang はマサチューセッツ工科大学の準教授であり，スタンフォード大学，カリフォルニア大学バークレー校，ロス・アラモス国立研究所，IBM アルマデン研究所等で研究業績をあげている．二人の研究論文は巻末の参考文献にそれぞれ 10 編以上リストアップされており，研究の第一線で活躍していることがわかる．

量子コンピュータや量子通信はコンピュータ技術や光ファイバ通信技術の未来の夢を示す方向として，またナノテクノロジーやフォトニクス技術の将来の進路を示す可能性の 1 つとして大いに期待され，科学技術先進諸国で多大のリソースが投入されて研究の推進がはかられている．この状況の中で，確固たる将来展望のもとに基本的事項をしっかりと記述した，本書のような書物の重要性が一層増

していると考えられる．このような意味で本書がわが国の学生，技術者を始め研究者や研究者を目指す多くの方々のお役に立つことができて，わが国のこの分野の研究発展に資することができれば，望外の幸せである．

翻訳に当たってはこの著者の姿勢を生かすよう留意したつもりである．さらに訳出にあたって著者のまえがきのある Web サイトに掲載された正誤にはすべて対応するとともに，翻訳時に見つかったその他の誤りもできるだけ修正しておいた．量子計算・量子情報の分野は数学・物理学・コンピュータ科学・通信工学・エレクトロニクス・フォトニクス・材料科学等，数多くの分野の境界領域であり，多くの分野の術語が入り交じって使われる．また，最先端分野に相応しくこの分野特有の新しい術語も生まれている．日本語への定着度が低い場合もあり，また特定の分野を背景とする読者は多少違和感を感じる場合もあるかも知れない．翻訳に伴ってこのような分野に見られる 1 つの問題点として，異なる英文術語が異なる領域で同一の和文術語に対応する場合がある．二三の例をあげると，基底（空間の base，対数の base，準位の ground），交換（commute，swap，exchange），可逆（invertible，reversible，reciprocal），指数（index，exponent），限界（bound，limit）等がある．文脈から判断できるようにするとともに，誤解のないように英術語を併記したところも多い．また和文と異なり英文での「以上」，「以下」はその数を含まない場合が多いことを付記しておく．

翻訳に当たって多くの方々にお世話になった．石原直氏，磯崎秀樹氏，向井孝彰氏，山本喜久氏に深く感謝する．また高柳英明氏，森田雅夫氏を始め NTT 物性科学基礎研究所の方々と NTT コミュニケーション科学基礎研究所の方々に多くの点で有益なご意見を頂いた．心からお礼を申し上げる．最後になったが出版に関してお世話になったオーム社出版部の方々に感謝する．

2004 年 12 月

訳者しるす

# 目　次

# 第I巻，第III巻目次

## 第I巻 — 量子力学とコンピュータ科学 —



## 第III巻 — 量子通信・情報処理と誤り訂正 —

# 用語と記号

量子計算と量子情報分野で共通に使われる用語と記号には，2 つあるいはそれ以上の意味を持つものがある．混乱を避けるためにここではこれら頻繁に使われる用語や記号を集め，本書での用法を併記する．

## 線形代数と量子力学

全ベクトル空間は特に断らない限り有限次元と仮定する．多くの場合にこの制約は不必要であるか，あるいは若干のテクニカルな操作により取り除くことができる．しかし一般にこの制約を設けることにより容易に理解することができ，結果を応用する際に用途が狭まることはない．

オペレータ (演算子，作用素，operator) $A$ が**正のオペレータ** であるということは，すべての $|\psi\rangle$ に対して $\langle\psi|A|\psi\rangle \geq 0$ となることである．また**正の定符号オペレータ** $A$ とは $|\psi\rangle \neq 0$ に対して $\langle\psi|A|\psi\rangle > 0$ となるオペレータである．オペレータの台 (support) は核 (kernel) と直交するベクトル空間であると定義される．これは Hermite オペレータ (Hermitian operator) に対して固有値が 0 でないオペレータの固有ベクトルが形成するベクトル空間を意味している．

記号 $U$（および，常時ではないがときどき $V$ も）は総称的にユニタリーオペレータ (unitary operator) またはユニタリー行列 (unitary matrix) を表すのに用いる．$H$ は通常量子論理ゲートの 1 つである Hadamard ゲート を表すのに用いるが，ときどき量子システムのハミルトニアン (Hamiltonian) を表す．この意味の違いは文脈より明らかである．

ベクトルは時に応じて，例えば

$$\begin{bmatrix} 1 \\ 2 \end{bmatrix} \tag{0.1}$$

のような列形式で書かれ，別のときには読み易いように行形式 (1, 2) で書くこともある．後者は列ベクトルの略記法と理解してほしい．通常，q ビットとして用いられる 2 準位システムに対して状態 $|0\rangle$ をベクトル (1, 0) で表し，状態 $|1\rangle$ を (0, 1) で表す．また我々は Pauli の $\sigma$ 行列 (Pauli $\sigma$ matrix) を通常用いられる通りに定義する．次に述べる「よく用いられる量子ゲートと回路記号」の項を参照されたい．最も重要なことは Pauli の $\sigma_z$ 行列に対する慣行は $\sigma_z|0\rangle = |0\rangle$，$\sigma_z|1\rangle = -|1\rangle$ であり，一部の物理学者の直観と逆になっている（通常コンピュータ科学者や数学者はそうしない）．この不一致の原因は物理学者は $\sigma_z$ の $+1$ 固有状態をいわゆる「励起状態」と規定し，多くの人がこれを本書で採用した $|0\rangle$ ではなく $|1\rangle$ と表すのが自然だと考えるからである．我々の選択は線形代数の行列要素における通常の指数と一致するものであり，$\sigma_z$ の第 1 列と $|0\rangle$ に及ぼす $\sigma_z$ の作用とを一致させ，第 2 列を $|1\rangle$ に及ぼす作用と一致させる．この選択は量子計算と量子情報の分野を通じて広く用いられている．Pauli の $\sigma$ 行列に対する通常の記号 $\sigma_x$，$\sigma_y$，$\sigma_z$ に加えて，これらの代わりに記号 $\sigma_1$，$\sigma_2$，$\sigma_3$ および $2 \times 2$ の単位行列 $\sigma_0$ を用いることも便利である．しかし，我々は $\sigma_0$，$\sigma_1$，$\sigma_2$，$\sigma_3$ に代えてそれぞれ記号 $I$，$X$，$Y$，$Z$ を頻繁に用いる．

## 情報理論と確率

優れた情報理論家にふさわしく特に断らない限り対数は**常に** 2 を基底とする．$\log(x)$ は 2 を基底とする対数を表し，稀にしか使わないが $\ln(x)$ は自然対数を表す．**確率分布**(probability distribution) という用語は $p_x \geq 0$ かつ $\sum_x p_x = 1$ であるような実数 $p_x$ の有限集合を表す．正のオペレータ $B$ に対する正のオペレータ $A$ の相対エントロピー は $S(A \,\|\, B) \equiv \mathrm{tr}(A \log A) - \mathrm{tr}(A \log B)$ で定義される．

# その他

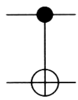
$\oplus$ は 2 を法とする和 を表す．本書を通じて '$z$' は [zed] と発音する．

# よく用いられる量子ゲートと回路記号

量子回路の設計に有用なユニタリー変換を表すのに，幾つかの図式的な記号がよく使われる．読者の便宜を図るためにそれらを集めて示しておく．ユニタリー変換の行と列は，$00\ldots0$，$00\ldots1$，から $11\ldots1$ というように左から右へ，上から下へと並べられ，最後の数字が最も重要でないビットを表す．$e^{i\pi/4}$ は $i$ の平方根であり，したがって $\pi/8$ ゲートは，Pauli-$Z$ ゲートの平方根である位相ゲートの平方根である．

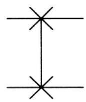
| | | |
|---|---|---|
| **Hadamard ゲート** | $H$ | $\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ |
| **Pauli-$X$ ゲート** | $X$ | $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ |
| **Pauli-$Y$ ゲート** | $Y$ | $\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$ |
| **Pauli-$Z$ ゲート** | $Z$ | $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ |
| **位相ゲート** | $S$ | $\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$ |
| **$\pi/8$ ゲート** | $T$ | $\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$ |

**制御 NOT ゲート**



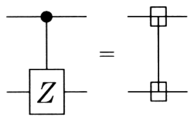
$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

**交換ゲート**



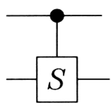
$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

**制御 $Z$ ゲート**



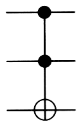

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$

**制御位相ゲート**



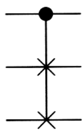

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & i \end{bmatrix}$$

**Toffoli ゲート**



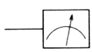
$$\begin{bmatrix} 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&0&0&0&1\\ 0&0&0&0&0&0&1&0 \end{bmatrix}$$

**Fredkin ゲート**
**（制御交換ゲート）**



$$\begin{bmatrix} 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&0&1&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&0&0&0&1 \end{bmatrix}$$

**測定**



$|0\rangle$ と $|1\rangle$ への射影

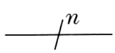
**q ビット**

単一 q ビットの配線
（時間は左から右へ経過）

**古典ビット**

単一の古典ビットの配線

**$n$ 個の q ビット**




$n$ 個の q ビットの配線

# 第II部

# 量子計算

# 第4章　量子回路

計算理論は従来純粋数学のテーマとして，ほとんどすべて抽象的思考で研究されてきた．これでは主要点を外すことになる．コンピュータは物理的対象であり，計算は物理プロセスである．コンピュータが計算できるものできないものを決めるのは，物理学法則のみであり，純粋数学ではない．　— David Deutsch

コンピュータ科学は数学のように，他の科学とは何か異なったものになるであろう．そこでは正確に知ることのできない自然法則に代わって，証明できる人工的な法則が扱われる．　— Donald Knuth

深遠な真実の反対側にも，もう 1 つの深遠な真実があるかも知れない．　— Niels Bohr

本章から量子計算を詳しく扱う第 II 部が始まる．本章では量子計算の基本原理を発展させ，洗練された量子計算を記述する普遍的言語である量子回路の基本的ブロック構成を確立する．続く 2 つの章ではこれらの回路を用いて，現在知られている 2 つの基本的量子アルゴリズムを作り上げる．5 章では量子 Fourier 変換とその応用である位相推定，位数発見および素因数分解について述べる．6 章では量子探索アルゴリズムとその応用であるデータベース探索，および **NP** 完全問題の解の数え上げと高速化について述べる．7 章ではいつの日か量子計算を実験的に実現する方法について議論する．量子計算で非常に興味ある 2 つの問題，つまり量子雑音と量子誤り訂正については，量子計算以外の広い興味も考慮して，本書の第 III 部まで延ばすことにする．

本章で導入する主要概念は 2 つある．第 1 に量子計算の基本的モデルである量子回路モデルを詳しく説明する．第 2 に少数ゲートの集合が**普遍的**であること，つまりおよそ如何なる量子計算でもこれらのゲートだけで表現できることを示す．その途上で機会を見て量子計算の多くの基礎的結果について述べる．本章の最初として 4.1 節で量子アルゴリズムを概観し，知られているアルゴリズムとその構築に係わる統合化技術に焦点を絞る．4.2 節では単一 q ビット演算を詳しく研究する．単一 q ビット演算は単純であるが実例やテクニックを構築する豊かな活動の場を提供し，その詳細を理解することが必須である．4.3 節では多 q ビットの**制御ユニタリー演算** (controlled unitary operation) の実行方法，4.4 節では量子回路モデルで測定を記述する方法を議論する．次にこれらの要素を組み合わせて，4.5 節で普遍性定理とその証明を示す．量子計算のすべての基礎的要素に関するまとめを 4.6 節で行い，モデルの変形の可能性や古典コンピュータと量子コンピュータの計算能力の関係に関する重要な疑問について議論する．本章の結論として 4.7 節で実際の量子システムの**シミュレーション**を行う，重要で啓発的な量子計算の応用について述べる．

本書の中で多分この 4 章は達成すべき演習を高密度に含み，最も訓練の要素が強い章なので，その理由を説明しておく必要があろう．計算の量子回路モデルにおける基本要素を取得することは極めて易しいが，もし量子アルゴリズムの設計というさらに困難な問題を目指すならば，多数の簡単な結果やテクニックが第 2 の天性となるまで理解吸収する必要がある．この理由でそのような能力を取得するために本章では例示主体のアプローチを取り，それに詳細に応えるよう読者に求めている．それほど集中せずにどちらかといえば表面的な量子計算の基本要素に関する概説が望みならば，4.6 節まで飛ばしてもよい．

## 4.1　量子アルゴリズム

量子コンピュータは何の役に立つか？ 我々はみんな計算問題を解くコンピュータのリソース不足にいつも欲求不満を持っている．実際のところ古典コンピュータ上で解けない興味ある問題が多いが，その理由は原理上解決不可能だからではなく，問題の現実的解を求めるのに天文学的リソースを要するからである．

量子コンピュータの華々しい将来像は，古典コンピュータで解くには法外なリ

ソースが必要な問題を計算可能にする，新しいアルゴリズムを提供することにある．この見通しを満たす量子アルゴリズムのクラスが本書の執筆時点で 2 つ存在する．最初のクラスは素因数分解や離散対数問題を解く注目すべきアルゴリズムを含む，Shor の**量子 Fourier 変換** (quantum Fourier transform) に基づくものであり，最良の古典アルゴリズムに比べて**指数関数的**な著しい高速化を実現する．第 2 のアルゴリズムクラスは**量子探索** (quantum search) を行う Grover のアルゴリズムに基づくものである．これはそれほど著しくはないが，それでも最良の古典アルゴリズムに比べて，**2 乗**の顕著な高速化を実現する．量子探索アルゴリズムが重要なのは古典アルゴリズムで探索ベースの技術が広く使われており，多くの事例で古典アルゴリズムを高速の量子アルゴリズムに直接変更することができるからである．

図 4.1 は例示的応用も含めて本書執筆時点における量子アルゴリズムの現状知識を整理した概略図である．図の上端には当然量子 Fourier 変換と量子探索アルゴリズムがくる．この図で特に興味があるのは量子計数アルゴリズムである．このアルゴリズムは量子探索と Fourier 変換アルゴリズムを巧妙に組み合わせて，古典コンピュータよりも早く探索問題の解の数を推定するのに使える．

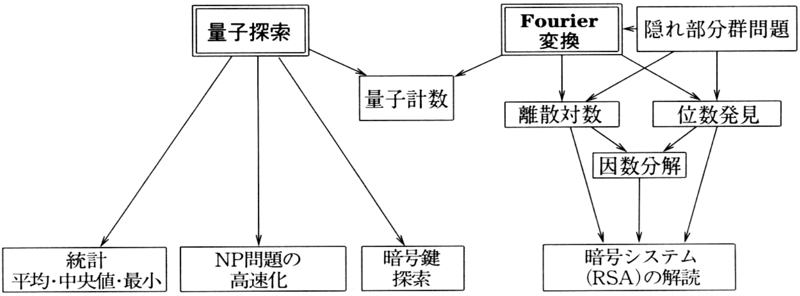



**図 4.1:** 主要な量子アルゴリズムとその関連性．有名な応用も含む．

量子探索アルゴリズムには多くの潜在的応用があるが，ここには一部のみを示した．これを使って順序付けしていないデータの集合から，例えば最小の要素のような統計を古典コンピュータよりも早く取り出すことができる．これを使うと **NP** のある種の問題 — 特に解の直接探索が最良のアルゴリズムと考えられている問題 — に対するアルゴリズムを高速化できる．最後にこれは広く使われる DES (Data Encryption Standard) のような暗号システムの鍵探索を高速化するのに

使える．これらをはじめその他の応用について 6 章で説明する．

量子 Fourier 変換にも多くの興味ある応用がある．これを使って離散対数問題や素因数分解が解ける．これらの結果によって今度は量子コンピュータが，RSA 暗号システムを含めて現在使われている最も一般的暗号システムの多くを打ち破ることができる．また Fourier 変換は数学の重要な問題である — 周期関数の周期を見出す問題を一般化した — 隠れ部分群を見出す問題に密接関連していることがわかる．素因数分解や離散対数に対する高速量子アルゴリズムも含めて量子 Fourier 変換とその幾つかの応用を 5 章で説明する．

古典アルゴリズムよりも良い量子アルゴリズムはなぜ少ししか知られていないのか？ 良い量子アルゴリズムを見つけることは難しそうであるというのが答である．この理由は少なくとも 2 つある．第 1 は古典的であれ量子的であれアルゴリズム設計は容易い仕事ではない！ アルゴリズムの歴史が示すところでは，2 つの数の積のように明らかに非常に簡単な問題に対してでも，最適に近いアルゴリズムを見つけるにはかなりの発明の才が求められることが多い．良い量子アルゴリズムを見出すには，最良の古典アルゴリズムよりも**より良い**量子アルゴリズムが求められるという制約がもう 1 つあるので，2 重に難しい．良い量子アルゴリズムを見出すのが困難な第 2 の理由は，我々の直観が量子的世界よりも古典的世界に良く適応していることである．生来の直観を使って問題を考えると，我々が見つけるアルゴリズムは古典アルゴリズムになる．良い量子アルゴリズムを見つけるには特別の洞察と特別の秘訣が必要なのである．

量子アルゴリズムをさらに研究するのは次章まで延ばすことにして，本章では量子アルゴリズムを記述する効率的で強力な言語である，量子回路言語— 計算手続きを記述する要素の集まり — について述べる．この構成によりアルゴリズムのコストを，必要なゲート総数とか回路の深さというようなもので定量化することができる．回路言語にはアルゴリズム設計を簡単にし，概念を容易に理解できる秘訣という道具箱も付いている．

## 4.2　単一 q ビット演算

我々の量子計算用の道具箱を発展させるのに，全量子システム中で最も単純な単一 q ビットの演算から始める．単一 q ビットゲートは 1.3.1 項（第 I 巻）で導

入した．そこで学んだことを手早く復習してみよう．これを進めるには本書まえがきに続く「用語と記号」欄の回路記号を参照すると役に立つ．

単一 q ビットは $|a|^2 + |b|^2 = 1$ を満たす 2 つの複素数パラメータを持つベクトル $|\psi\rangle = a|0\rangle + b|1\rangle$ である．q ビットへの演算はそのノルムを保存しなければならないので，$2 \times 2$ のユニタリー行列で与えられる．もちろん最も重要なものの 1 つが Pauli の行列であり，便宜上ここに再掲しておく：

$$X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}; \quad Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}; \quad Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{4.1}$$

今後 Hadamard ゲート（$H$ と表す），位相ゲート（$S$ と表す），$\pi/8$ ゲート（$T$ と表す）の 3 つのゲートも大きな役割を演じる：

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}; \quad S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}; \quad T = \begin{bmatrix} 1 & 0 \\ 0 & \exp(i\pi/4) \end{bmatrix}. \tag{4.2}$$

心に留めておくべき有用な代数式が 2 つある．それは $H = (X + Z)/\sqrt{2}$ と $S = T^2$ である．$T$ ゲートの定義に $\pi/4$ が現れるのになぜ $\pi/8$ ゲートと呼ぶのか不思議に思うかも知れない．この理由は重要でないグローバル位相を除いて，$T$ は対角要素が $\exp(\pm i\pi/8)$ であるゲートに等しいという理由で，単に歴史的に $\pi/8$ ゲートと呼ばれてきたからである．

$$T = \exp(i\pi/8) \begin{bmatrix} \exp(-i\pi/8) & 0 \\ 0 & \exp(i\pi/8) \end{bmatrix}. \tag{4.3}$$

それにもかかわらずある点でこの名称は不適切なので，我々はこれを $T$ ゲートと呼ぶ．

単一 q ビット $a|0\rangle + b|1\rangle$ は単位球上の点 $(\theta, \varphi)$ として可視化できることを思い出そう．ここで $a = \cos(\theta/2)$, $b = e^{i\varphi}\sin(\theta/2)$ であり，状態全体の位相は観測可能でないので $a$ は実数とすることができる．この表示を Bloch 球表現，ベクトル $(\cos\varphi\sin\theta,\ \sin\varphi\sin\theta,\ \cos\theta)$ は Bloch ベクトルと呼ぶ．直観を助けるためにこの描像を今後しばしば用いる．

**演習 4.1:** 演習 2.11（第 I 巻）をまだ解いていなければここで解いて，Pauli の行列の固有ベクトルを求めよ．異なる Pauli の行列の正規化固有ベクトルに対応する Bloch 球上の点を求めよ．

Pauli 行列の指数関数から $\hat{x}$, $\hat{y}$, $\hat{z}$ 軸の回りの**回転オペレータ** (rotation operator) という 3 つのユニタリー行列の便利なクラスが生まれ，次式で定義される：

$$R_x(\theta) \equiv e^{-i\theta X/2} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}X = \begin{bmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix} \tag{4.4}$$

$$R_y(\theta) \equiv e^{-i\theta Y/2} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}Y = \begin{bmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix} \tag{4.5}$$

$$R_z(\theta) \equiv e^{-i\theta Z/2} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}Z = \begin{bmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{bmatrix}. \tag{4.6}$$

**演習 4.2:** $x$ を実数として，$A$ を $A^2 = I$ なる行列とする．

$$\exp(iAx) = \cos(x)I + i\sin(x)A \tag{4.7}$$

を示せ．この結果を使って式 (4.4)〜(4.6) を証明せよ．

**演習 4.3:** グローバル位相を除いて $\pi/8$ ゲートが $T = R_z(\pi/4)$ を満たすことを示せ．

**演習 4.4:** Hadamard ゲート $H$ を $R_x$ 回転，$R_z$ 回転，およびある $\varphi$ に対する $e^{i\varphi}$ の積として示せ．

もし $\hat{n} = (n_x, n_y, n_z)$ が実の 3 次元単位ベクトルとすると，前の式を一般化して $\hat{n}$ 軸の回りの回転 $\theta$ を次式で定義できる．

$$R_{\hat{n}}(\theta) \equiv \exp(-i\theta\hat{n}\cdot\vec{\sigma}/2) = \cos\left(\frac{\theta}{2}\right)I - i\sin\left(\frac{\theta}{2}\right)(n_xX + n_yY + n_zZ), \tag{4.8}$$

ここで $\vec{\sigma}$ は Pauli の行列の 3 成分ベクトル $(X,\ Y,\ Z)$ を表す．

**演習 4.5:** $(\hat{n}, \vec{\sigma})^2 = I$ を証明せよ．またこれを用いて式 (4.8) を証明せよ．

**演習 4.6:（回転の Bloch 球による解釈）** $R_{\hat{n}}(\theta)$ を回転オペレータと呼ぶ 1 つの理由は次の事実による．これを証明せよ．単一 q ビットが Bloch ベクトル $\vec{\lambda}$ で表される状態を持つとする．このときこの状態に対する回転 $R_{\hat{n}(\theta)}$ の効果は，Bloch 球の $\hat{n}$ 軸の回りに角度 $\theta$ だけ回転することである．回転行列において一見不思議に見える因子 2 の理由がこの事実により説明できる．

**演習 4.7:** $XYX = -Y$ を示せ．これを使って $XR_y(\theta)X = R_y(-\theta)$ を証明せよ．

**演習 4.8:** 任意の単一 q ビット ユニタリーオペレータは実数 $\alpha, \theta$ および 3 次元実数単位ベクトル $\hat{n}$ に対して次のように書ける．

$$U = \exp(i\alpha)R_{\hat{n}}(\theta). \tag{4.9}$$

(1) これを証明せよ．

(2) Hadamard ゲート $H$ を与える $\alpha$, $\theta$, $\hat{n}$ の値を見出せ．

(3) 位相ゲート $S$ を与える $\alpha$, $\theta$, $\hat{n}$ の値を見出せ．

$$S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}. \tag{4.10}$$

単一 q ビットに働く任意のユニタリーオペレータは，q ビットのグローバル位相シフトと合わせて，回転の組合せとして多くの方法で書くことができる．次の定理は任意の q ビット回転を表現する方法を提供するもので，後で制御演算に応用する際に特に有用になる．

**定理 4.1:（単一 q ビットに対する *Z-Y* 分解）** $U$ は単一 q ビットに働くユニタリー変換であるとする．このとき

$$U = e^{i\alpha}R_z(\beta)R_y(\gamma)R_z(\delta) \tag{4.11}$$

を満たす実数 $\alpha$, $\beta$, $\gamma$, $\delta$ が存在する．

**証明**　$U$ はユニタリーなので $U$ の行と列は正規直交しており，次式を満たす実数 $\alpha,\ \beta,\ \gamma,\ \delta$ が存在する：

$$U = \begin{bmatrix} e^{i(\alpha-\beta/2-\delta/2)}\cos\frac{\gamma}{2} & -e^{i(\alpha-\beta/2+\delta/2)}\sin\frac{\gamma}{2} \\ e^{i(\alpha+\beta/2-\delta/2)}\sin\frac{\gamma}{2} & e^{i(\alpha+\beta/2+\delta/2)}\cos\frac{\gamma}{2} \end{bmatrix}. \tag{4.12}$$

回転行列の定義と行列積から式 (4.11) は直ぐに導ける．□

**演習 4.9:** 単一 q ビットのユニタリーオペレータがなぜ式 (4.12) の形に書けるか説明せよ．

**演習 4.10:（回転の $X$-$Y$ 分解）** $R_z$ の代わりに $R_x$ を用いて定理 4.1 と類似の分解を与えよ．

**演習 4.11:** $\hat{m}$ と $\hat{n}$ は直交する実数の 3 次元単位ベクトルとする．$\alpha,\ \beta_k,\ \gamma_k$ を適切に選ぶと，任意の単一 q ビットユニタリー変換 $U$ は次のように書けることを示せ．

$$U = e^{i\alpha}R_{\hat{n}}(\beta_1)R_{\hat{m}}(\gamma_1)R_{\hat{n}}(\beta_2)R_{\hat{m}}(\gamma_2)\ldots. \tag{4.13}$$

定理 4.1 が有用である理由は次の一見不思議な系 (corollary) にあり，次節で説明するようにこれが制御多 q ビットユニタリー演算を構成する鍵となる．

**系 4.2:** $U$ は単一 q ビットに働くユニタリーゲートとする．そのとき単一 q ビットに働くユニタリーオペレータ $A,\ B,\ C$ が存在して，$ABC = I$ および $U = e^{i\alpha}AXBXC$ を満たす．ここで $\alpha$ は全体の位相因子である．

**証明**　定理 4.1 の記号において $A \equiv R_z(\beta)R_y(\gamma/2)$，$B \equiv R_y(-\gamma/2)R_z(-(\delta+\beta)/2)$，$C \equiv R_z((\delta-\beta)/2)$ とおく．

$$ABC = R_z(\beta)R_y\left(\frac{\gamma}{2}\right)R_y\left(\frac{-\gamma}{2}\right)R_z\left(-\frac{\delta+\beta}{2}\right)R_z\left(\frac{\delta-\beta}{2}\right) = I \tag{4.14}$$

である．$X^2 = I$ であり演習 4.7 を用いると，

$$XBX = XR_y\left(-\frac{\gamma}{2}\right)XXR_z\left(-\frac{\delta+\gamma}{2}\right)X = R_y\left(\frac{\gamma}{2}\right)R_z\left(\frac{\delta+\beta}{2}\right). \tag{4.15}$$

したがって

$$AXBXC = R_z(\beta)R_y\left(\frac{\gamma}{2}\right)R_y\left(\frac{\gamma}{2}\right)R_z\left(\frac{\delta+\beta}{2}\right)R_z\left(\frac{\delta-\beta}{2}\right) \tag{4.16}$$

$$= R_z(\beta)R_y(\gamma)R_z(\delta). \tag{4.17}$$

したがって，要求された通り $U = e^{i\alpha}AXBXC$ および $ABC = I$ となる． □

**演習 4.12:** Hadamard ゲートに対して $A$, $B$, $C$, $\alpha$ を与えよ．

**演習 4.13:（回路の同等性）** よく知られた等式を使って目視により回路を単純化できれば便利である．次の 3 つの等式を証明せよ：

$$HXH = Z;\ HYH = -Y;\ HZH = X. \tag{4.18}$$

**演習 4.14:** 前の演習を使ってグローバル位相を除いて $HTH = R_x(\pi/4)$ なることを示せ．

**演習 4.15:（単一 q ビット演算の構成）** Bloch 表現は 2 つの回転効果を可視化する良い方法である．

(1) 軸 $\hat{n}_1$ の回りに角度 $\beta_1$ だけ回転し，次に軸 $\hat{n}_2$ の回りに角度 $\beta_2$ だけ回転すると，それは全体として軸 $\hat{n}_{12}$ の回りの角度 $\beta_{12}$ の回転として次式で与えられることを証明せよ．

$$c_{12} = c_1c_2 - s_1s_2\hat{n}_1\cdot\hat{n}_2, \tag{4.19}$$

$$s_{12}\hat{n}_{12} = s_1c_2\hat{n}_1 + c_1s_2\hat{n}_2 + s_1s_2\hat{n}_2\times\hat{n}_1, \tag{4.20}$$

ただし $c_i = \cos(\beta_i/2)$, $s_i = \sin(\beta_i/2)$, $c_{12} = \cos(\beta_{12}/2)$, $s_{12} = \sin(\beta_{12}/2)$ である．

(2) もし $\beta_1 = \beta_2$ および $\hat{n}_1 = \hat{z}$ ならばこれらの式は次のように簡単化されることを示せ：

$$c_{12} = c^2 - s^2\hat{z}\cdot\hat{n}_2, \tag{4.21}$$

$$s_{12}\hat{n}_{12} = sc(\hat{z}+\hat{n}_2) + s^2\hat{n}_2\times\hat{z}, \tag{4.22}$$

ただし $c = c_1$, $s = s_1$ である．

共通の単一 q ビットゲートに対する記号を図 4.2 に示す．量子回路の基本的性質である時間は左から右へ経過すること，配線は q ビットを表すこと，および「/」は q ビットの束を表すのに用いることを思い出して欲しい．

| | | |
|---|---|---|
| Hadamard ゲート | $-\boxed{H}-$ | $\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ |
| Pauli-$X$ ゲート | $-\boxed{X}-$ | $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ |
| Pauli-$Y$ ゲート | $-\boxed{Y}-$ | $\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$ |
| Pauli-$Z$ ゲート | $-\boxed{Z}-$ | $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ |
| 位相ゲート | $-\boxed{S}-$ | $\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$ |
| $\pi/8$ ゲート | $-\boxed{T}-$ | $\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$ |

**図 4.2:** 共通の単一 q ビットゲートの名称，記号およびユニタリー行列.

## 4.3　制御演算

「もし $A$ が真ならば，$B$ を実行せよ」. この形の**制御演算** (cotrolled operation) は古典的でも量子的でも計算に最も有用なものである．本節では基本演算で構成する量子回路を用いて，如何にして複雑な制御演算を実行するかを説明する．

制御演算の原型は制御 NOT (CNOT，controlled-NOT) であり，これは 1.2.1 項（第 I 巻）で出てきたものである．そのゲート — 制御 NOT ゲートと呼ぶ — は，**制御 q ビット** (control qubit) と**標的 q ビット** (target qubit) の 2 つの入力 q ビットを有する量子ゲートであることを思い出そう．その回路は図 4.3 に示す記号で表す．計算基底についていえば制御 NOT の操作は $|c\rangle|t\rangle \rightarrow |c\rangle|t \oplus c\rangle$，つまりもし制御 q ビットが $|1\rangle$ にセットされていれば標的 q ビットは反転し，そうでなければそのままに保たれる．したがって，計算基底「| 制御，標的 ⟩」において制御 NOT の行列表現は次のようになる．

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}. \tag{4.23}$$

一般に $U$ が任意の単一 q ビットユニタリー演算であるとする．**制御 $U$ 演算** (controlled-$U$ operation) とは 2 個の q ビット演算であり，制御 q ビットと標的 q ビットを有する．制御 q ビットが 1 ならば標的 q ビットに $U$ を適用し，そうでなければ標的 q ビットはそのままにする．つまり $|c\rangle|t\rangle \to |c\rangle U^c|t\rangle$ である．制御 $U$ 演算は図 4.4 の回路で表現する．

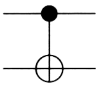


**図 4.3:** 制御 NOT ゲートの回路表現．上の線は制御 q ビット，下の線は標的 q ビットを表す．

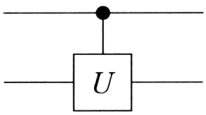
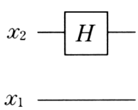
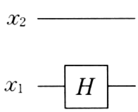



**図 4.4:** 制御 $U$ 演算．上の線は制御 q ビット，下の線は標的 q ビットを示す．もし制御 q ビットが 1 ならば標的に $U$ が適用され，そうでなければそのままに保たれる．

**演習 4.16:（多 q ビットゲートの行列表現）** 計算基底において，左の回路に対する $4 \times 4$ ユニタリー行列は何か？　また計算基底における右の回路のユニタリー行列は何か？

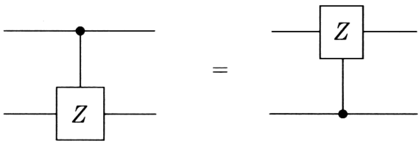



**演習 4.17:（制御 $Z$ ゲートから制御 NOT を構成）** 1 個の制御 $Z$ ゲートと，制御 q ビットと標的 q ビットを規定する 2 つの Hadamard ゲートを用いて制御 NOT ゲートを構成せよ．ここで制御 $Z$ ゲートは計算基底に対して次のユニタリー行列で表される．

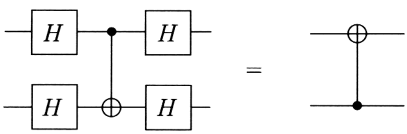
$$
\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}.
$$

**演習 4.18** 次の関係を示せ.



**演習 4.19:（密度行列への制御 NOT の動作）** 制御 NOT は単純な並べ替えであって，その密度行列 $\rho$ に対する動作は行列要素の並べ替えである．計算基底においてこの動作を明示的に書き表せ.

**演習 4.20:（制御 NOT 基底変換）** 理想的な古典ゲートと異なり，理想的量子ゲートは（電気技術者の言う）「高インピーダンス入力」を持っていない．実際「制御」と「標的」の役割には任意性があり，デバイスがどんな計算基底で動作すると考えるかに依存する．これまで制御 NOT ゲートが計算基底に関してどのように振る舞うかを記述してきた．この記述で制御 q ビットの状態は変化しない．しかし，もし異なる基底で動作すると，制御 q ビットは**変化する**．「標的」q ビットの状態に依存して，制御 q ビットの位相が反転することを示そう！ 次の関係を示せ.



基底状態 $|\pm\rangle \equiv (|0\rangle \pm |1\rangle)/\sqrt{2}$ を導入し，上の回路の同等性を使って最初の q ビットが制御で次の q ビットが標的である制御 NOT の効果が次のように表されることを示せ.

$$|+\rangle|+\rangle \rightarrow |+\rangle|+\rangle, \tag{4.24}$$

$$|-\rangle|+\rangle \rightarrow |-\rangle|+\rangle, \tag{4.25}$$

$$|+\rangle|-\rangle \rightarrow |-\rangle|-\rangle, \tag{4.26}$$

$$|-\rangle|-\rangle \rightarrow |+\rangle|-\rangle. \tag{4.27}$$

したがって，この新しい基底を用いると標的 q ビットの状態は変化しない一方，もし標的が最初 $|-\rangle$ ならば制御 q ビットの状態が反転し，そうでなければそのままに保持される．つまり，この基底では標的と制御の役割が本質的に入れ替わる！

我々の当面の目標は単一 q ビット演算と制御 NOT ゲートだけを用いて，任意の単一 q ビット $U$ に対する制御 $U$ 演算を如何に実現するかを理解することである．我々の戦略は系 4.2 を用いて $U = e^{i\alpha}AXBXC$ に分解して 2 つの手続きに分けて進める．

第 1 ステップは制御 q ビットで制御して，標的 q ビットに位相シフト $\exp(i\alpha)$ を適用する．つまり，もし制御 q ビットが $|0\rangle$ なら標的 q ビットはそのまま，制御 q ビットが $|1\rangle$ なら標的 q ビットに位相シフト $\exp(i\alpha)$ を適用する．単一 q ビットのユニタリーゲートのみを使ってこの演算を実行する回路を図 4.5 の右側に示す．この回路が正しい動作することを確かめるには，右側回路の効果が次のように表されることを確認する：

$$|00\rangle \rightarrow |00\rangle, \quad |01\rangle \rightarrow |01\rangle, \quad |10\rangle \rightarrow e^{i\alpha}|10\rangle, \quad |11\rangle \rightarrow e^{i\alpha}|11\rangle, \tag{4.28}$$

これはまさに左側の制御演算に求められたものに他ならない．

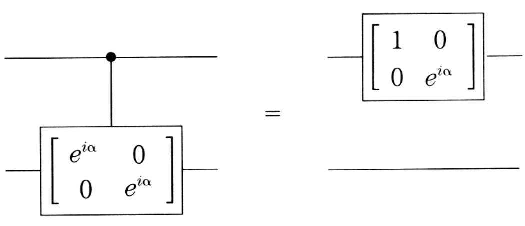


**図 4.5:** 2 つの q ビットに対する制御位相シフトゲートと等価回路．

これにより図 4.6 に示すように制御 $U$ 演算の構築を完成させることができる．この回路の動作を理解するために，系 4.2 より $U$ は $U = e^{i\alpha}AXBXC$ の形に書

けることを思い出そう．ここで $A$, $B$, $C$ は $ABC = I$ なる単一 q ビット演算である．制御 q ビットが 1 ならば第 2 - q ビットに演算 $e^{i\alpha}AXBXC = U$ を適用し，制御 q ビットが 1 でなければ演算 $ABC = I$ を第 2 - q ビットに適用する — つまり変化をさせない．したがってこの回路が制御 $U$ 演算を実現する．

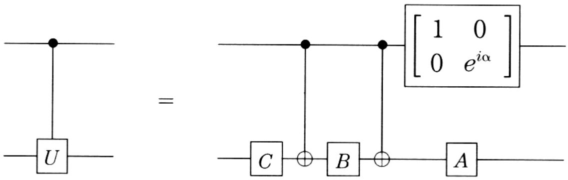



**図 4.6:** 単一 q ビットに対する制御 $U$ 演算 $U$ を実行した回路．図中で $\alpha, A, B,$ および $C$ は式 $U = \exp(i\alpha)AXBXC$, $ABC = I$ を満たす．

これで単一 q ビットがセットされた場合の条件付けの仕方がわかったが，多 q ビットへの条件付けはどうか？ 我々はすでに多 q ビットの条件付けの例を 1 つ知っている．Toffoli ゲートは制御ビットである最初の 2 つのビットが 1 にセットされる条件のもとで，標的ビットである第 3 - q ビットが反転する．一般に $n+k$ 個の q ビットがあるとし，$U$ は $k$ 個の q ビットの働くユニタリーオペレータであるとする．このとき制御演算 $C^n(U)$ を次式で定義する．

$$C^n(U)|x_1x_2\dots x_n\rangle|\psi\rangle = |x_1x_2\dots x_n\rangle U^{x_1x_2\dots x_n}|\psi\rangle, \tag{4.29}$$

ここで $U$ のベキ指数 $x_1x_2\dots x_n$ はビット $x_1$, $x_2, \dots, x_n$ の**積**を意味する．つまり，もし最初の $n$ 個の q ビットがすべて 1 ならば最後の $k$ 個の q ビットに $U$ を適用し，そうでなければ何もしない．このような条件付き演算は便利なので，そのために図 4.7 に示す特別の回路記号を導入する．簡単のためにこれ以降 $k=1$ と仮定する．それ以上の $k$ でも本質的に同じ方法で扱えるが，$k \geq 2$ に対しては $k$ 個の q ビットに対する任意の演算をどう実行するか，というまだわかっていない複雑さが加わることになる．

$U$ を単一 q ビットのユニタリーオペレータ，$V$ を $V^2 = U$ となるように選んだユニタリーオペレータであるとする．このとき演算 $C^2(U)$ は図 4.8 に示した回路で実現できる．

**演習 4.21:**　図 4.8 が $C^2(U)$ を実現することを証明せよ．

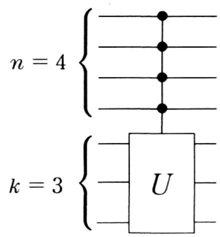



**図 4.7:** $C^n(U)$ 演算に対する回路表現例．ここで $U$ は $k$ 個の q ビットへのユニタリーオペレータであり，$n = 4$, $k = 3$ の場合を示す．

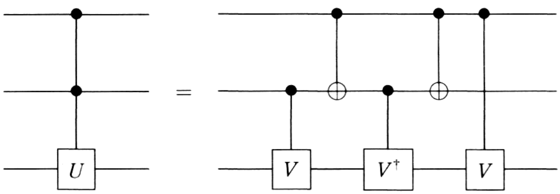



**図 4.8:** $C^2(U)$ ゲートに対する回路．$V$ は $V^2 = U$ を満たす任意のユニタリーオペレータ．$V \equiv (1-i)(I+iX)/2$ の特別な場合が Toffoli ゲートに相当する．

**演習 4.22:** $C^2(U)$ ゲートは（任意の単一 q ビットのユニタリー $U$ に対して）たかだか 8 個の単一 q ビットゲートと 6 個の制御 NOT ゲートで構築できることを証明せよ．

**演習 4.23:** 制御 NOT と単一 q ビットゲートだけを使って，$U = R_x(\theta)$ と $U = R_y(\theta)$ に対する $C^1(U)$ ゲートを組み立てよ．この回路で単一 q ビットゲートの数を 3 つから 2 つに減らせるか？

よく知っている Toffoli ゲートは，$C^2(U)$ 演算の特に重要な特別のケースであり，$C^2(X)$ に相当する．$V \equiv (1-i)(I+iX)/2$ と定義し，$V^2 = X$ に留意すると，図 4.8 が 1 - q ビットおよび 2 - q ビット演算で表した Toffoli ゲートを実現していることがわかる．古典的観点からこれは注目すべき結果である．問題 3.5（第 I 巻）より 1 ビットと 2 ビットの古典的可逆ゲートだけでは，Toffoli ゲートを — あるいは一般に普遍的計算を — 実現するには不十分であったことを思い出そう．これに対して量子回路では，1 および 2 - q ビットの可逆ゲートで Toffoli ゲートを実現することができ，したがって結局普遍的計算ができることが証明される．

我々は究極的に任意のユニタリー演算が任意の良い近似で Hadamard ゲート，

位相ゲート，制御 NOT ゲートおよび $\pi/8$ ゲートだけから構成できることを示す．Toffoli ゲートが非常に便利なのでこのゲートセットだけから如何に構成できるかを知ることは興味深い．図 4.9 は Hadamard，位相，制御 NOT，$\pi/8$ のゲートだけから構成した Toffoli ゲートに対する簡単な回路である．

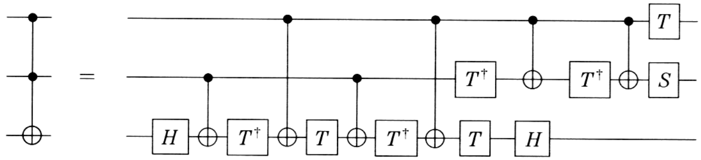



**図 4.9:** Hadamard，位相，制御 NOT，$\pi/8$ のゲートを用いて構成した Toffoli ゲート

**演習 4.24:** 図 4.9 が Toffoli ゲートを実現することを証明せよ．

**演習 4.25:（Fredkin ゲート構成）** Fredkin ゲート（制御交換）は次の変換を実行することを思い出そう．

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}. \tag{4.30}$$

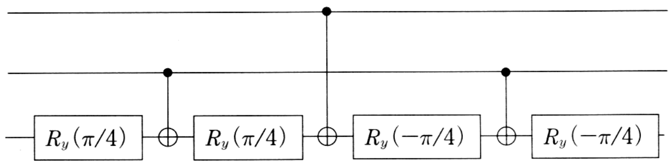
(1) 3 つの Toffoli ゲートを用いて Fredkin ゲートを構成する量子回路を与えよ．（ヒント：交換ゲート構造を考えよ — 一度に 1 つのゲートを制御できる．）

(2) 最初と最後の Toffoli ゲートは制御 NOT ゲートで置き換えられることを示せ．

(3) 中央の Toffoli ゲートを図 4.8 の回路で置き換え，6 個の 2 - q ビットゲートだけで構成された Fredkin ゲートを作れ．

(4) 5 個の 2 - q ビットゲートだけで，より簡単な構成を作れるか？

**演習 4.26:** 次の回路は Toffoli ゲートと相対位相だけが異なることを示せ．つまりこの回路は入力 $|c_1,\ c_2,\ t\rangle$ を $e^{i\theta(c_1,c_2,t)}|c_1,\ c_2,\ t\oplus c_1\cdot c_2\rangle$ に変換する．ここで $e^{i\theta(c_1,\ c_2,\ t)}$ はある相対位相因子である．このようなゲートは相対位相を除いて Toffoli ゲートと同じであるが，Toffoli ゲートよりも直接実現し易く実験に便利なことがある．




**演習 4.27:** 制御 NOT と Toffoli ゲートだけを使って，次の変換を実行する量子回路を構成せよ．この種の部分的な周期的並べ替え演算は 7 章で役に立つ．

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}. \tag{4.31}$$

$U$ を任意の単一 q ビットユニタリー演算として，我々のレパートリにある既存ゲートを用いて，$C^n(U)$ を如何にして構成できるか？ このタスクを達成するための特に簡単な回路を図 4.10 に示す．この回路は 3 段階に分かれており，$(n-1)$ 個という少数の作業 q ビット — すべて状態 $|0\rangle$ から始まって $|0\rangle$ に終わる — を使っている．制御 q ビットは計算基底状態 $|c_1,\ c_2,\dots,c_n\rangle$ にあるとする．回路の第 1 段階は全制御ビット $c_1,\ c_2,\dots,c_n$ の AND をとり，積 $c_1\cdot c_2\dots c_n$ を作る．これを行うのに回路の最初のゲートで Toffoli ゲートを使って $c_1$ と $c_2$ の AND をとり，最初の作業 q ビットを $|c_1\cdot c_2\rangle$ に変える．次の Toffoli ゲートで $c_3$ と積 $c_1\cdot c_2$ の AND をとり第 2 作業 q ビットを $|c_1\cdot c_2\cdot c_3\rangle$ に変える．このように最後

の作業ビットが状態 $|c_1 \cdot c_2 \ldots c_n\rangle$ になるまで Toffoli ゲートの適用を続ける．次に最後の作業ビットが 1 にセットされていれば標的 q ビットに演算 $U$ を施す．つまり，もし $c_1$ から $c_n$ まですべてが 1 であるときにのみ $U$ を適用する．最後にこの回路の最終段階として最初の段階の逆を行いすべての作業ビットを最初の状態 $|0\rangle$ に戻す．したがって，全部の結果を組み合わせると，$c_1$ から $c_n$ までの全制御ビットが 1 のときにのみ標的 q ビットにユニタリーオペレータ $U$ を施すことができる．

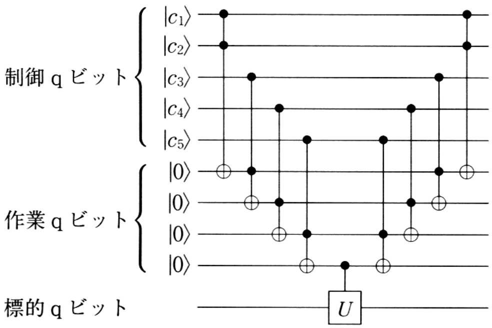



**図 4.10:** $n = 5$ に対する $C^n(U)$ 演算ネットワークの実現．

**演習 4.28:** $V$ がユニタリー，$U = V^2$ に対して図 4.10 と同様であるが作業ビットを使わずに $C^5(U)$ を構築せよ．制御 $V$ と制御 $V^\dagger$ ゲートを使ってよい．

**演習 4.29:** $O(n^2)$ 個の Toffoli ゲート，制御 NOT ゲートおよび単一 q ビットゲートを含み，作業ビットを使わずに $C^n(X)$ ゲート（$n > 3$）を実行する回路を見出せ．

**演習 4.30:** $U$ は単一 q ビットのユニタリー演算であるとする．$O(n^2)$ 個の Toffoli ゲート，制御 NOT ゲートおよび単一 q ビットゲートを含み，作業ビットを使わずに $C^n(U)$ ゲート（$n > 3$）を実行する回路を見出せ．

我々が考えてきた制御ゲートでは，制御ビットが **1** にセットされれば標的ビットへの条件付き動作がなされる．もちろん 1 に対しては何も特別なことはないが，制御ビットが 0 にセットされたときに条件付き動作が行われることを考えるのも有益である．例えば，第 1（制御）q ビットが 0 であるという条件で第 2（標的）

q ビットが反転するような，2 - q ビットゲートを作りたいとする．図 4.11 にこのゲートに対する回路記号とすでに使った記号で表した等価回路を示す．一般に q ビットが 0 のときという条件を示すのに白丸記号を用い，q ビットが 1 のときという条件を示すのに黒丸記号を用いる．

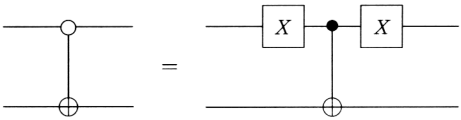



**図 4.11:** 第 1 - q ビットが 0 にセットされた条件下で第 2 - q ビットに NOT ゲートを実行する制御演算

3 つの制御 q ビットを含むもう少し手の込んだ慣用法の例を図 4.12 に示す．第 1 と第 3 の q ビットが 0 にセットされ第 2 の q ビットが 1 にセットされたときに，標的 q ビットに演算 $U$ が適用される．図の右側の回路が望みの演算を実現することが目視で容易にわかる．一般に 1 にセットされる条件の回路と 0 にセットされる条件の回路は，図に示すように $X$ ゲートを適切な場所に挿入することによって互いに変換できる．

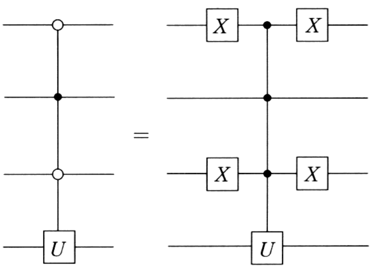



**図 4.12:** 制御 $U$ 演算と既知の回路要素で表した等価回路．第 1 と第 3 の q ビットが 0，第 2 の q ビットが 1 にセットされたときに，第 4 の q ビットに演算 $U$ が適用される．

もう 1 つの便利な慣用法は図 4.13 に示すように，制御 NOT ゲートに多重標的 q ビットを許すことである．これは自然な拡張であり，その記号の意味は制御 q ビットが 1 のときに，$\oplus$ 記号があるすべての q ビットが反転し，そうでなければ何も起きない．これを使うと，例えば置換のような古典的機能を実現するときや，10 章（第 III 巻）で見る量子誤り訂正回路の符号器・復号器で便利である．

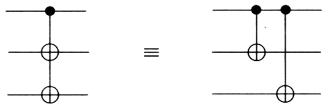


図 4.13: 多重標的ビットを持つ制御 NOT.

**演習 4.31（その他の等価な回路）** 添字はオペレータが作用するqビットを表し，$C$ はqビット1を制御qビット，qビット2を標的qビットとする制御NOTとする．次の等式を証明せよ：

$$CX_1C = X_1X_2 \tag{4.32}$$

$$CY_1C = Y_1X_2 \tag{4.33}$$

$$CZ_1C = Z_1 \tag{4.34}$$

$$CX_2C = X_2 \tag{4.35}$$

$$CY_2C = Z_1Y_2 \tag{4.36}$$

$$CZ_2C = Z_1Z_2 \tag{4.37}$$

$$R_{z,1}(\theta)C = CR_{z,1}(\theta) \tag{4.38}$$

$$R_{x,2}(\theta)C = CR_{x,2}(\theta). \tag{4.39}$$

## 4.4　測定

量子回路に用いられる最後の要素は，ほとんど暗黙にではあるが測定である．我々の回路では図4.14に示すように，計算基底における射影測定（2.2.5項：第I巻）を「測定器」の記号で表す．量子回路理論では一般の測定を表す特別な記号を使わないのが従来の慣行である．その理由は2章（第I巻）で説明したように，これらは常に補助qビットを用いたユニタリー変換に続く射影測定で表せるからである．

量子回路に関して心に留めておく価値がある2つの重要な原理がある．いずれの原理もどちらかというと自明なものであるが，非常に利用価値があるので早めに強調しておいたほうがよい．最初の原理は古典的な条件の付いた演算は量子的な条件付き演算に置き換えることができるというものである：

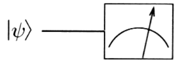



**図 4.14:** 単一 q ビット射影測定の記号．この回路では測定結果に対して何も行われないが，一般の量子回路では前の回路部分の測定結果に応じた**条件付き**で量子回路の後の部分を変化させることができる．そのような古典情報の使い方を 2 重線の配線で示す（ここには示されていない）．

**遅延測定の原理：**量子回路の途中にある測定は常に回路の最後に移すことができる．もし測定結果が回路の任意の段階で使われるならば，古典的制御演算は条件付き量子演算で置き換えることができる．

量子測定はしばしば量子回路の途中の段階で行われて，測定結果が次の量子ゲートの条件付き制御に使われる．図 1.13 (第 I 巻) のテレポーテーション回路のケースがこの例である．しかしこのような測定は**常に**回路の最後に動かすことができる．図 4.15 はすべての古典的条件付き演算を対応する条件付き量子演算で置き換えることにより，これを行う方法を示している．(もちろんこの変更で Alice から Bob へ古典情報が伝送されないので，この回路が「テレポーテーション」を実行するという解釈は一部失われるが，2 つの量子回路の総体的動作が同じであるのは明らかであり，そこが大事な点である.)

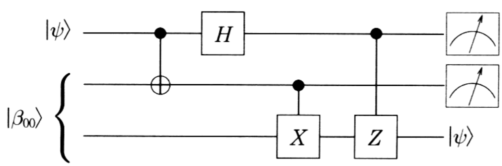



**図 4.15:** 測定が回路の途中でなく，最後で行われる量子テレポーテーション回路．図 1.13（第 I 巻）と同じく上の 2 - q ビットは Alice，下の q ビットは Bob のものを表す．

第 2 の原理はもっと明白であるが驚くほど便利である！

**暗黙測定の原理：**回路の最後にある終端されていない配線（測定されていない q ビット）は一般性を失うことなく測定されたものと仮定してよい．

なぜこれが正しいかを理解するために 2 個の q ビットだけを含む量子回路があるとし，最初の q ビットだけが回路の最後で測定されるとする．ここで観測され

る測定の統計は最初のqビットの縮約（簡約）した密度行列で完全に決められる．しかし第2-qビットについても測定がなされたとして，その測定により最初のqビットの測定統計が変化したとすれば驚くべきことである．第2-qビットの測定を実行することによって，第1-qビットの縮約した密度行列が影響を受けないことを演習4.32で証明してもらう．

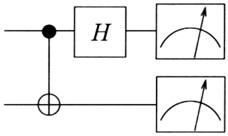
量子回路における測定を考えるときに心に留めておくべき重要なことは，量子世界と古典世界のインタフェースとしての役割の中で，測定は一般に非可逆演算であると考えられ，量子情報を破壊して古典情報で置き換えることになる．しかしある種の注意深く設計されたケースでは，テレポーテーションや量子誤り訂正（10章：第III巻）に鮮やかに見られるように，これは必ずしも正しくない．テレポーテーションと量子誤り訂正の共通点は，いずれの場合も測定結果は測定されるべき量子状態の正体について何の情報も示していないことである．測定が実際に可逆であるためには，被測定量子状態の情報を示してはならない — これが測定の一般的特徴であることを10章（第III巻）で示す．

**演習 4.32:** $\rho$ は2個のqビットシステムを記述する密度行列であるとし，第2のqビットを計算基底で射影測定をすると仮定する．$P_0 = |0\rangle\langle 0|$ と $P_1 = |1\rangle\langle 1|$ はそれぞれ第2-qビットの状態 $|0\rangle$ と $|1\rangle$ への射影であるとする．観測者が測定した後で観測結果について知らない場合に，測定後にシステムがとるであろう密度行列を $\rho'$ とする．次式を示せ．

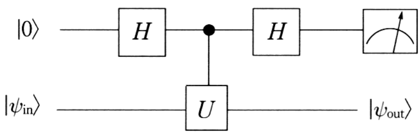
$$\rho' = P_0 \rho P_0 + P_1 \rho P_1. \tag{4.40}$$

また最初のqビットに対する縮約した密度行列はその測定で影響されないこと，つまり $\mathrm{tr}_2(\rho) = \mathrm{tr}_2(\rho')$ を示せ．

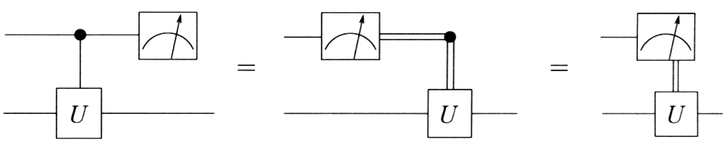
**演習 4.33:（Bell 基底での測定）** 量子回路モデルに対して規定した測定モデルは，計算基底に関して行う測定だけであった．しかし正規直交状態の完全集合で定義された，何か別の基底に関して測定したいこともある．この測定を行うには，測定したい基底から計算基底にユニタリー変換を行い，その後に測定を行えばよい．例えば次の回路はBell状態を基底とする測定を行うことを示せ．正確に言えば，この回路は対応するPOVM要素，つまりBell状態への4つの射影オペレータで実行された測定となることを示せ．対応する測定オペレータは何か？



**演習 4.34:（オペレータの測定）** 固有値 ±1 を有する単一 q ビットオペレータ $U$ があり，$U$ は Hermite オペレータでかつユニタリーであるとする．したがって，それは観測量であると共に量子ゲートであると見なせる．観測量 $U$ を測定するとする．つまり 2 つの固有値の一方を示す結果を得て，測定後の状態を対応する固有ベクトルにしたいとする．この量子回路を実現するにはどうするか？ 次の回路が $U$ の測定を実現することを示せ．




**演習 4.35:（制御と交換可能な測定）** 遅延測定の原理の結果は，被測定 q ビットが制御 q ビットならば，測定と量子ゲートは可換であるということである．図示すると次のようになる．（図中の 2 重線は古典ビットを表すことを思い出そう．）最初の等号を証明せよ．一番右の回路は測定結果を使って量子ゲートを古典的に制御することを表す便利な記号である．




## 4.5　普遍的量子ゲート

3.1.2 項（第 I 巻）で見たように少数のゲート（例えば AND, OR, NOT）だけを使って任意の古典的関数を計算できる．このようなゲート集合を古典計算に対する**普遍的**ゲートと呼ぶ．実際 Toffoli ゲートは古典計算で普遍的なので，量子回路は古典回路を包含している．同様な普遍性が量子計算に対しても成り立ち，これらのゲートだけを含む量子回路でどんなユニタリー演算でも任意の精度で近

似できるならば，そのゲート集合は**量子計算に普遍的**であるという．ここで量子計算に対する普遍性の 3 つの構成について述べる．これらの構成は互いのうえに成り立っており，その頂点には任意のユニタリー演算が Hadamard，位相，制御 NOT および $\pi/8$ ゲートを使って任意の精度で近似できるという証明が位置する．位相ゲートは 2 つの $\pi/8$ ゲートで構成できるのにこのリストになぜ位相ゲートが出てくるのかいぶかる向きもあるかも知れないが，10 章（第 III 巻）で述べる耐故障性構成に自然に現れるのでここに含めた．

最初の構成が示すのは任意のユニタリーオペレータが，2 つの計算基底状態が張る部分空間の中だけで有意に働くユニタリーオペレータの積で，**正確に**表現されることである．第 2 の構成では最初の構成と前項の結果を組み合わせて，任意のユニタリーオペレータが単一 q ビットゲートと制御 NOT ゲートを用いて**正確に**表現できることを示す．第 3 の構成は第 2 の構成と，Hadamard，位相および $\pi/8$ ゲートを使って，単一 q ビット演算を任意の精度で近似できるという証明とを組み合わせたものである．これは逆に Hadamard，位相，制御 NOT および $\pi/8$ ゲートを使って，任意のユニタリー演算が任意の精度で近似できることを意味している．

この構成は効率 — つまり与えられたユニタリー変換を幾つのゲートで構成できるか（多項式数か指数関数的数か）？ — についてほとんど言及していない．4.5.4 項において，近似するのに指数関数的に多数のゲートを必要とするユニタリー変換が**存在する**ことを示す．もちろん量子計算のゴールは効率良く**実行できる**興味あるユニタリー変換の族 (family) を見出すことである．

**演習 4.36:** 2 つの 2 ビット数 $x, y$ を 4 を法として加える量子回路を構築せよ．つまり変換 $|x,\ y\rangle \rightarrow |x,\ x+y \bmod 4\rangle$ を実行する回路を見出せ．

### 4.5.1　普遍的な 2 準位ユニタリーゲート

$d$ 次元 Hilbert 空間で働くユニタリー行列 $U$ を考える．本項では $U$ を **2 準位ユニタリー行列**(two-level unitary matrix) — つまりベクトルの 2 つまたはそれ以下の成分のみに有意に働くユニタリー行列 — の積に分解する方法を説明する．この分解の裏にある重要な概念を理解するために，$U$ が $3 \times 3$ の場合を考える．

$U$ が次の形をとるとする：

$$U = \begin{bmatrix} a & d & g \\ b & e & h \\ c & f & j \end{bmatrix}. \tag{4.41}$$

次式を満たす 2 準位ユニタリー行列 $U_1, \ldots, U_3$ を見出すのが目標である.

$$U_3 U_2 U_1 U = 1. \tag{4.42}$$

これより

$$U = U_1^\dagger U_2^\dagger U_3^\dagger. \tag{4.43}$$

$U_1$, $U_2$, $U_3$ はすべて 2 準位ユニタリー行列とすると，それらの逆行列 $U_1^\dagger$, $U_2^\dagger$, $U_3^\dagger$ も 2 準位ユニタリー行列であることが容易にわかる．したがって，もし式 (4.42) を示すことができれば $U$ を 2 準位ユニタリー行列に分解する方法を示したことになる.

次の手続きで $U_1$ を構築する：　もし $b = 0$ ならば

$$U_1 \equiv \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}. \tag{4.44}$$

もし $b \neq 0$ ならば,

$$U_1 \equiv \begin{bmatrix} \frac{a^*}{\sqrt{|a|^2+|b|^2}} & \frac{b^*}{\sqrt{|a|^2+|b|^2}} & 0 \\ \frac{b}{\sqrt{|a|^2+|b|^2}} & \frac{-a}{\sqrt{|a|^2+|b|^2}} & 0 \\ 0 & 0 & 1 \end{bmatrix}. \tag{4.45}$$

いずれの場合も $U_1$ は 2 準位ユニタリー行列であり行列積をとると次式を得る.

$$U_1 U = \begin{bmatrix} a' & d' & g' \\ 0 & e' & h' \\ c' & f' & j' \end{bmatrix}. \tag{4.46}$$

注目すべきは 2 行 1 列の行列要素が 0 である点である．ここで行列内の他の要素はプライムをつけた記号で表しているが，その実際の値は重要でない.

同様の手続きを踏んで $U_2U_1U$ の左下隅の要素が0になるように2準位行列 $U_2$ を決める．つまりもし $c'=0$ ならば，

$$U_2 \equiv \begin{bmatrix} a'^* & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \tag{4.47}$$

一方もし $c' \neq 0$ ならば，

$$U_2 \equiv \begin{bmatrix} \frac{a'^*}{\sqrt{|a'|^2+|c'|^2}} & 0 & \frac{c'^*}{\sqrt{|a'|^2+|c'|^2}} \\ 0 & 1 & 0 \\ \frac{c'}{\sqrt{|a'|^2+|c'|^2}} & 0 & \frac{-a'}{\sqrt{|a'|^2+|c'|^2}} \end{bmatrix} \tag{4.48}$$

と置く．いずれの場合も行列積を実行すると次式が得られる．

$$U_2U_1U = \begin{bmatrix} 1 & d'' & g'' \\ 0 & e'' & h'' \\ 0 & f'' & j'' \end{bmatrix}. \tag{4.49}$$

$U$, $U_1$, $U_2$ はユニタリーなので $U_2U_1U$ はユニタリーであり，したがって $U_2U_1U$ の第1行はノルム1でなければならないので $d''=g''=0$ である．最終的に次のように置ける．

$$U_3 \equiv \begin{bmatrix} 1 & 0 & 0 \\ 0 & e''^* & f''^* \\ 0 & h''^* & j''^* \end{bmatrix}. \tag{4.50}$$

$U_3U_2U_1U=I$ を証明するのは容易であり，したがって $U=U_1^\dagger U_2^\dagger U_3^\dagger$ となり，これは $U$ を2準位ユニタリー行列に分解したものである．

一般に $U$ が $d$-次元空間で働くとすると，$3\times 3$ の場合と同様に行列 $U_{d-1}U_{d-2}\ldots U_1U$ の左上の要素が1で，第1行と第1列の他の要素がすべて0となるような，2準位ユニタリー行列 $U_1,\ldots,U_{d-1}$ を見出すことができる．この手続きを $U_{d-1}U_{d-2}\ldots U_1U$ の右下隅の $(d-1)\times(d-1)$ のユニタリー部分行列に対して繰り返し，同様の手続きを続けると最終的に任意の行列 $d\times d$ ユニタリー行列が次のように書ける．

$$U = V_1 \ldots V_k, \tag{4.51}$$

ここで行列 $V_i$ は 2 準位ユニタリー行列であり，$k \leq (d-1)+(d-2)+\ldots+1 = d(d-1)/2$ である．

**演習 4.37:** 次の変換行列を 2 準位ユニタリー行列の積に分解せよ．これは次章で詳しく学ぶ量子 Fourier 変換の特別なケースである．

$$\frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{bmatrix}. \tag{4.52}$$

上の結果の系 (corollary) は，$n$ 個の q ビットシステムに働く任意のユニタリー行列は，たかだか $2^{n-1}(2^n-1)$ 個の 2 準位ユニタリー行列の積で書くことができる．特別なユニタリー行列に対してもっと効率の良い分解が見つかるかも知れないが，次の演習にあるように，$(d-1)$ 個以下の 2 準位ユニタリー行列の積に分解することができない行列が存在する．

**演習 4.38:** $d-1$ 個よりも少ない 2 準位ユニタリー行列の積に分解できない $d \times d$ ユニタリー行列 $U$ が存在することを証明せよ．

### 4.5.2 普遍的な単一 q ビットゲートと制御 NOT ゲート

これまでに示したように $d$ 次元の Hilbet 空間の任意のユニタリー行列は 2 準位ユニタリー行列の積で書くことができる．次に単一 q ビットゲートと制御 NOT ゲートとを使って，$n$ - q ビットの状態空間における任意の 2 準位ユニタリー演算を実現できることを示そう．これらの結果を組み合わせると，単一 q ビットと制御 NOT ゲートを使って $n$ - q ビットへの任意のユニタリー演算を実現することができ，したがってこれらは量子計算に対して普遍的であることがわかる．

$U$ は $n$ 個の q ビット量子コンピュータに働く 2 準位ユニタリー行列であるとする．特に $U$ は計算基底 $|s\rangle$ と $|t\rangle$ が張る空間で有意に働くとする．ここで $s = s_1 \ldots s_n$ と $t = t_1 \ldots t_n$ は $s$ と $t$ の 2 進数展開である．$\tilde{U}$ は $U$ の有意のユニタリーな

$2 \times 2$ 部分行列であるとすると，$\tilde{U}$ は単一 q ビットへのユニタリーオペレータと考えられる．

当面のゴールは単一 q ビットと制御 NOT ゲートを使って $U$ を実行する回路を作り上げることである．このために **Grey 符号**を用いる．異なる 2 進数 $s$ と $t$ があるとする．$s$ と $t$ をつなぐ **Gray 符号**は $s$ から始まり $t$ に終わる一連の 2 進数で，隣り合う要素の差を正確に 1 ビットとする．例えば $s = 101001$, $t = 110011$ とすると Gray 符号は次のようになる．

$$\begin{matrix} 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 \end{matrix} \tag{4.53}$$

$s$ と $t$ をつなぐ Gray 符号の要素を $g_1$ から $g_m$ とする．ここで $g_1 = s$, $g_m = t$ である．$s$ と $t$ はたかだか $n$ 個の位置の違いなので $m \leq n+1$ であるような Gray 符号を常に見つけることができる．

$U$ を実行する量子回路の基本的考え方は，状態変化 $|g_1\rangle \to |g_2\rangle \to \cdots \to |g_{m-1}\rangle$ を生じる一連のゲートを実行し，次に $g_{m-1}$ と $g_m$ との間で異なる 1 つのビットを標的 q ビットとして制御 $\tilde{U}$ 演算を実行し，次に最初のステップの逆の変換 $|g_{m-1}\rangle \to |g_{m-2}\rangle \to \cdots \to |g_1\rangle$ を行って元に戻す．この各々のステップは本章でこれまでに明らかにした演算を使って容易に実現することができて，最終結果が $U$ を実現したものになる．

この実行過程をもう少し詳しく述べると次のようになる．最初のステップで状態 $|g_1\rangle$ と $|g_2\rangle$ を入れ替える．$g_1$ と $g_2$ は $i$ 番目の数字が異なるとすると，$g_1, g_2$ の他の q ビットの値が同じという条件で，$i$ 番目の q ビットに制御ビット反転を実行して入れ替える．次に $|g_2\rangle$ と $|g_3\rangle$ を入れ替える制御演算を行う．このような操作を $|g_{m-2}\rangle$ と $|g_{m-1}\rangle$ を入れ替えるまで続ける．この $m-2$ 回の連続した演算の結果，次の演算が実行される：

$$|g_1\rangle \to |g_2\rangle, \tag{4.54}$$

$$|g_2\rangle \to |g_3\rangle, \tag{4.55}$$

$$|g_3\rangle \to |g_4\rangle, \tag{4.56}$$

$$\cdots\cdots\cdots$$

$$|g_{m-2}\rangle \to |g_{m-1}\rangle, \tag{4.57}$$

他のすべての計算基底状態はこの一連の演算操作で変化しない．次に $g_{m-1}$ と $g_m$ が $j$ 番目のビットで異なるとすると，$g_m$ と $g_{m-1}$ の両方に現れる他の q ビットが同じ値を持つという条件で，$j$ 番目の q ビットに制御 $\tilde{U}$ 演算を適用する．最後の段階は $g_{m-1}$ と $g_{m-2}$ を置き換え，$g_{m-2}$ と $g_{m-3}$ を置き換え等々，最後に $g_2$ と $g_1$ を置き換えるという具合に最初に行った置き換えを元に戻す．

この手続きを簡単な例で示す．次の 2 準位ユニタリー変換を実行するとする．

$$U = \begin{bmatrix} a & 0 & 0 & 0 & 0 & 0 & 0 & c \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ b & 0 & 0 & 0 & 0 & 0 & 0 & d \end{bmatrix}. \tag{4.58}$$

ここで $a,\ b,\ c,\ d$ は $\tilde{U} \equiv \begin{bmatrix} a & c \\ b & d \end{bmatrix}$ がユニタリー行列となるような任意の複素数である．$U$ は状態 $|000\rangle$ と $|111\rangle$ だけに有意に働くことに留意する．000 と 111 をつなぐ Gray 符号は：

$$\begin{array}{ccc} A & B & C \\ 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{array}. \tag{4.59}$$

これから図 4.16 に示すように要求される回路を読み出す．最初の 2 つのゲートは $|000\rangle$ と $|011\rangle$ が置き換わるように状態を混ぜ合わせる．次に 2 番目と 3 番目

の q ビットが状態 $|11\rangle$ にあるという条件で，状態 $|011\rangle$ と $|111\rangle$ にある最初の q ビットに演算 $\tilde{U}$ を適用する．混ぜ合わせた状態を元に戻して，置き換わった $|011\rangle$ が $|000\rangle$ に戻ることを確認する．

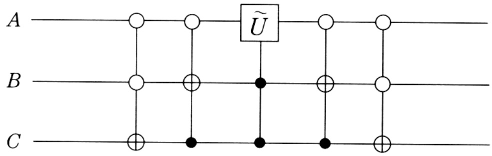



**図 4.16:** 式 (4.58) で定義される 2 準位ユニタリー演算回路の実現．

一般の場合に戻って，2 準位ユニタリー演算 $U$ を実行するには，$|g_1\rangle$ と $|g_{m-1}\rangle$ の置き換えとその逆操作を行うのに，たかだか $2(n-1)$ 回の制御演算を必要とすることがわかる．この各々の制御演算を実行するには $O(n)$ 個の単一 q ビットゲートと制御 NOT ゲートが必要であり，制御 $\tilde{U}$ 演算にも $O(n)$ 個のゲートが要る．したがって $U$ の実行には $O(n^2)$ 個の単一 q ビットと制御 NOT ゲートが必要になる．前項で見たように $n$ 個の q ビットの $2^n$ 次元状態空間に働く任意のユニタリー行列は，$O(2^{2n}) = O(4^n)$ 個の 2 準位ユニタリー演算の積で書ける．これらの結果を組み合わせると，$n$ 個の q ビットに働く任意のユニタリー演算は，$O(n^2 4^n)$ 個の単一 q ビットと制御 NOT ゲートを含む回路を使って実現できることがわかる．明らかにこの構成は恐ろしく効率の良い量子回路を提供するものではない！ しかし指数関数的ゲート数の実行を必要とするユニタリー演算が存在するという意味で，この構成は最適に近いものであることを 4.5.4 項で示す．したがって，速い量子アルゴリズムを見つけるには，明らかに普遍的構成と異なるアプローチが必要である．

**演習 4.39:** 単一 q ビット演算と制御 NOT 演算を用いて次の変換を実現する量子回路を見出せ．

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & a & 0 & 0 & 0 & 0 & c \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & b & 0 & 0 & 0 & 0 & d \end{bmatrix}, \tag{4.60}$$

ここで $\tilde{U} \equiv \begin{bmatrix} a & c \\ b & d \end{bmatrix}$ は任意の $2 \times 2$ ユニタリー行列である．

### 4.5.3　普遍的演算の離散的集合

制御 NOT と単一 q ビットユニタリー演算が量子計算の普遍的組み合わせとなることを前項で証明した．残念ながら誤り耐性を持つ形で，これら全ゲートを実行する直接的方法は知られていないが，幸い普遍的量子計算を実行するのに使えるゲートの離散的集合が本項で見出せる．10 章（第 III 巻）では量子誤り訂正符号を用いて，誤り耐性を有する形でこれらのゲートを実行する方法を示す．

#### ユニタリーオペレータの近似

ユニタリー演算の集合は連続なので，ゲートの離散的集合では明らかに任意のユニタリー演算を**正確**に実行することはできない．その代わりに離散的集合を使って，任意のユニタリー演算が**近似**できることがわかっている．この働きを理解するために，まずユニタリー演算の近似の意味を知る必要がある．$U$ と $V$ は同じ状態空間における 2 つのユニタリーオペレータであるとする．$U$ は実行したい目標とするユニタリーオペレータ，$V$ は実際に実行される（近似的な）ユニタリーオペレータである．$U$ の代わりに $V$ が実行されたときの**誤差**を次式で定義する：

$$E(U,V) \equiv \max_{|\psi\rangle} \|(U-V)|\psi\rangle\|, \tag{4.61}$$

ここで max は状態空間のすべての正規化された量子状態 $|\psi\rangle$ に関する最大値である．コラム 4.1 に示すようにこの誤差の尺度は次のように解釈される： もし $E(U,V)$ が小さければ，任意の初期状態 $|\psi\rangle$ に対して状態 $V|\psi\rangle$ に実行された任意の測定は，$U|\psi\rangle$ の測定と近似的に同じ測定統計を与える．正確に言えば，もし $M$ が任意の POVM における POVM 要素であり，$U$（または $V$）を初期状態 $|\psi\rangle$ に適用したときにその結果を得る確率を $P_U$（または $P_V$）とすると

$$|P_U - P_V| \le 2E(U,V). \tag{4.62}$$

したがってもし $E(U,V)$ が小さければ $U$ か $V$ のいずれが実行されるかに関わりなく，測定結果は同じ確率で生じる．またコラム 4.1 では，もし他の一連のゲート $U_, \ldots, U_m$ を近似する目的で一連のゲート $V_1, \ldots, V_m$ を実行したとすると，誤差はたかだか線形で相加することを示す．

$$E(U_m U_{m-1} \ldots U_1,\ V_m V_{m-1} \ldots V_1) \le \sum_{j=1}^{m} E(U_j,\ V_j). \tag{4.63}$$

式 (4.62) と (4.63) の近似は非常に便利なものである．仮に $U_1$ から $U_m$ の $m$ 個のゲートを含む量子回路を実行しようとする．不幸にしてゲート $U_j$ を $V_j$ で近似するしかできない．近似回路から得られる異なる測定結果の確率が正しい確率と誤差 $\Delta > 0$ 以下であるためには，式 (4.62), (4.63) の結果により $E(U_j, V_j) \le \Delta/(2m)$ であれば十分である．

**コラム 4.1: 量子回路の近似**

量子システムが状態 $|\psi\rangle$ から出発してユニタリー演算 $U$ か，あるいはユニタリー演算 $V$ を実行すると想定する．その後で測定を行う．$M$ を測定に関連する POVM 要素とし，演算 $U$（または $V$）を実行したときに測定結果を得る確率を $P_U$（または $P_V$）とする．このとき

$$|P_U - P_V| = |\langle\psi|U^\dagger M U|\psi\rangle - \langle\psi|V^\dagger M V|\psi\rangle|. \tag{4.64}$$

$|\Delta\rangle \equiv (U - V)|\psi\rangle$ とする．簡単な代数計算と Cauchy-Schwarz の不等式

より

$$|P_U - P_V| = |\langle\psi|U^\dagger M|\Delta\rangle + \langle\Delta|MV|\psi\rangle|. \tag{4.65}$$
$$\leq |\langle\psi|U^\dagger M|\Delta\rangle| + |\langle\Delta|MV|\psi\rangle| \tag{4.66}$$
$$\leq \||\Delta\rangle\| + \||\Delta\rangle\| \tag{4.67}$$
$$\leq 2E(U,\ V). \tag{4.68}$$

この不等式 $|P_U - P_V| \leq 2E(U,\ V)$ は，誤差 $E(U,\ V)$ が小さければ測定結果間の確率の差も小さいことを定量的に表現する．

ある一連のゲート $U_1,\ U_2, \ldots, U_m$ を近似するために，ゲート $V_1,\ V_2, \ldots, V_m$ を実行するとする．一連の不完全なゲート全体により生じる誤差は，たかだか各ゲートの誤差の総和であることがわかる．

$$E(U_m U_{m-1} \ldots U_1,\ V_m V_{m-1} \ldots V_1) \leq \sum_{j=1}^{m} E(U_j, V_j). \tag{4.69}$$

これを証明するために $m = 2$ の場合から出発する．ある状態 $|\psi\rangle$ に対して

$$E(U_2U_1,\ V_2V_1) = \|(U_2U_1 - V_2V_1)|\psi\rangle\| \tag{4.70}$$
$$= \|(U_2U_1 - V_2U_1)|\psi\rangle + (V_2U_1 - V_2V_1)|\psi\rangle\|. \tag{4.71}$$

三角不等式 $\||a\rangle + |b\rangle\| \leq \||a\rangle\| + \||b\rangle\|$ を用いると，

$$E(U_2U_1, V_2V_1) \leq \|(U_2 - V_2)U_1|\psi\rangle\| + \|V_2(U_1 - V_1)|\psi\rangle\| \tag{4.72}$$
$$\leq E(U_2,\ V_2) + E(U_1,\ V_1). \tag{4.73}$$

これが求める結果である．一般の $m$ に対する結果は帰納法で得られる．

### Hadamard + 位相 + 制御 NOT + $\pi/8$ ゲートの普遍性

ゲートの離散的集合による任意のユニタリー演算の近似を調べる段階になった．両方とも普遍的な離散的ゲートの 2 つの集合を考える．最初の集合は Hadamard，位相，制御 NOT，$\pi/8$ ゲートよりなり，これを**標準集合**と呼ぶ．これらのゲー

トによる耐故障性を持つ構成を10章（第III巻）で示すが，これらは例外的に単純な普遍的構成になる．次に考える第2のゲート集合はHadamardゲート，位相ゲート，制御NOTゲートおよびToffoliゲートで構成される．これらを使っても耐故障性の動作ができるが，これらに対する普遍性の証明と耐故障性構成は多少魅力に欠ける．

普遍性の証明を始めるに当たりまずHadamardと$\pi/8$ゲートを使って，任意のqビットユニタリー演算を任意の精度で近似できる証明を示す．ゲート$T$と$HTH$を考える．$T$は重要でないグローバル位相を除いてBloch球上で$\hat{z}$軸の回りに$\pi/4$ラディアンだけ回転すること相当し，$HTH$はBloch球上で$\hat{x}$軸の回りに$\pi/4$ラディアン回転することに相当する（演習4.14）．この2つの演算を組み合わせるとグローバル位相を除いて

$$
\begin{aligned}
&\exp\left(-i\frac{\pi}{8}Z\right)\exp\left(-i\frac{\pi}{8}X\right) \\
&= \left[\cos\frac{\pi}{8}I - i\sin\frac{\pi}{8}Z\right]\left[\cos\frac{\pi}{8}I - i\sin\frac{\pi}{8}X\right] &(4.74)\\
&= \cos^2\frac{\pi}{8}I - i\left[\cos\frac{\pi}{8}(X+Z) + \sin\frac{\pi}{8}Y\right]\sin\frac{\pi}{8}. &(4.75)
\end{aligned}
$$

これはBloch球上で$\vec{n} = (\cos\frac{\pi}{8},\ \sin\frac{\pi}{8},\ \cos\frac{\pi}{8})$に沿った単位ベクトル$\hat{n}$を軸として，$\cos(\theta/2) \equiv \cos^2\frac{\pi}{8}$で定義される角度$\theta$だけ回転することを表す．つまりHadamardゲートと$\pi/8$ゲートだけを使って$R_{\vec{n}}(\theta)$を構成できる．さらにこの$\theta$は$2\pi$の無理数倍であることが示せる．後者の事実の証明は本書の範囲を少し超えているので，章末の「歴史と参考資料」欄を見て欲しい．

次に$R_{\hat{n}}(\theta)$を繰り返し適用すると，任意の回転$R_{\hat{n}}(\alpha)$を任意の精度で近似できることを示す．これを確かめるために，希望精度を$\delta > 0$，$2\pi/\delta$より大きい整数を$N$とする．$\theta_k \in [0, 2\pi)$，$\theta_k = (k\theta) \bmod 2\pi$なる$\theta_k$を定義する．このとき鳩の巣箱の原理 (pigeonhole principle) [1]によれば，$1, \ldots, N$の範囲内に，$|\theta_k - \theta_j| \le 2\pi/N < \delta$であるような異なる$j$と$k$が存在する．一般性を失うことなく$k > j$と仮定すると$|\theta_{k-j}| < \delta$となる．$j \neq k$であり$\theta$は$2\pi$の無理数倍なので，$\theta_{k-j} \neq 0$でなければならない．その結果$l$が変化したときに一連の$\theta_{l(k-j)}$は間隔$[0, 2\pi)$を完全に満たし，一連の隣り合う要素の間隔が$\delta$以上になることはない．任意の$\epsilon' > 0$に対して次式を満たす$n$が存在する．

[1]訳注： Dirichletの引き出し論法，あるいは部屋割り論法とも呼ぶ．

$$E(R_{\hat{n}}(\alpha), R_{\hat{n}}(\theta)^n) < \frac{\epsilon'}{3}. \tag{4.76}$$

**演習 4.40:** 任意の $\alpha$ と $\beta$ に対して次式を示し，これを用いて式 (4.76) を示せ．

$$E(R_{\hat{n}}(\alpha), R_{\hat{n}}(\alpha+\beta)) = |1-\exp(i\beta/2)|. \tag{4.77}$$

単一 q ビット演算を Hadamard ゲートと $\pi/8$ ゲートで，任意精度の近似ができることを証明する段階にきた．任意の $\alpha$ に対して簡単な代数計算で，

$$HR_{\hat{n}}(\alpha)H = R_{\hat{m}}(\alpha), \tag{4.78}$$

ここで $\hat{m}$ は $(\cos\frac{\pi}{8},\ -\sin\frac{\pi}{8},\ \cos\frac{\pi}{8})$ 方向の単位ベクトルである．これから

$$E(R_{\hat{m}}(\alpha),\ R_{\hat{m}}(\theta)^n) < \frac{\epsilon'}{3}. \tag{4.79}$$

しかし演習 4.11 から単一 q ビットに働く任意のユニタリー $U$ は，重要でないグローバル位相変化を除いて $\hat{n}$ 軸と $\hat{m}$ 軸の回りの回転の有限な積で，次のように書ける．

$$U = R_{\hat{n}}(\beta_1)R_{\hat{m}}(\gamma_1)R_{\hat{n}}(\beta_2)R_{\hat{m}}(\gamma_2)\ldots\ . \tag{4.80}$$

ここで $\hat{n}$ と $\hat{m}$ を固定すると，ユニタリー変換 $U$ を表すのに要する回転行列 $R$ の数 $c$ は $U$ に依存せずに定数となる．式 (4.76), (4.79) および連鎖不等式 (4.63) より，適当な正の整数 $n_1,\ n_2,\ n_3,\ldots$ に対して

$$E(U,\ R_{\hat{n}}(\theta)^{n_1}HR_{\hat{n}}(\theta)^{n_2}HR_{\hat{n}}(\theta)^{n_3}\ldots) < c\epsilon'/3. \tag{4.81}$$

**補遺:** 式 (4.76) において $n$ の選び方を変えて右辺が $\epsilon/c$ となるようにすると，式 (4.79) の右辺は $\epsilon/c$，式 (4.81) の右辺は $\epsilon$ で与えられる．

つまり，任意の単一 q ビットユニタリーオペレータ $U$ と任意の $\epsilon = c\epsilon'/3 > 0$ が与えられると，Hadamard ゲートと $\pi/8$ ゲートのみを用いて $\epsilon$ 以下で $U$ を近似することができる．

任意の単一 q ビットのユニタリーオペレータを $\pi/8$ および Hadamard ゲートにより近似できるので，4.5.2 項の議論より次のようにゲート $m$ 個よりなる任意の量子回路を近似することができる．制御 NOT または単一 q ビットユニタリー

ゲートの $m$ 個のゲートを含む量子回路が与えられると，それを Hadamard，制御 NOT および $\pi/8$ ゲートで近似できる（位相ゲートがあると後で耐故障性を持つ近似ができるが，いまの普遍性の議論にそれは厳密には必要ない）．全回路に対して $\epsilon$ の精度を望むなら，上の手続きにより各単一ビットユニタリーオペレータを $\epsilon/m$ 以下の精度で近似して，連鎖不等式 (4.63) を適用すれば全回路に対して $\epsilon$ の精度が得られる．

ゲートの離散的集合を用いたこの量子回路の近似手続きはどれくらい効率的か？これは重要な疑問である．例えば，任意の単一 q ビットユニタリー演算を距離 $\epsilon$ 以内で近似するには，離散的集合から $\Omega(2^{1/\epsilon})$ 個のゲートを必要とする．次に前の段落で考えた $m$ 個の量子ゲートを近似するには，$\Omega(m2^{m/\epsilon})$ 個のゲートが必要となり，元の回路サイズに比べて指数関数的増加になる！ 幸いなことに収束の割合はこれよりはるかに良い．直観的には一連の角度 $\theta_k$ が間隔 $[0, 2\pi)$ を多かれ少なかれ一様に「満たす」ことがもっともらしいので，任意の単一 q ビットゲートを近似するには，離散的集合からおよそ $\Theta(1/\epsilon)$ 個のゲートを持ってくる必要がある．任意の単一 q ビットゲートを近似するに必要なゲート数に対してこの推定を使うと，$\epsilon$ の精度で $m$ 個のゲートを近似するに必要な数は $\Theta(m^2/\epsilon)$ となる．これは元の回路サイズ $m$ の 2 乗の増加であり多くの応用にはこれで十分であろう．

しかし注目すべきはもっと早く収束することが証明できる．付録 C で証明する **Solovay-Kitaev の定理** (Solovay-Kitaev theorem) によれば任意の単一 q ビットゲートは離散的集合から取った $O(\log^c(1/\epsilon))$ 個のゲートによって精度 $\epsilon$ で近似されることが示される．ここで $c$ はほぼ 2 に近い定数である．したがって Solovay-Kitaev の定理は，離散的集合から $O(m \log^c(m/\epsilon))$ 個のゲートを持ってくると，$m$ 個の制御 NOT と単一 q ビットユニタリーゲートを含む回路が精度 $\epsilon$ で近似できることを意味する．これは元の回路サイズに比べて対数多項式倍の増加に収まっており，事実上すべての応用に対して容認できるものである．

以上をまとめると，制御 NOT と任意の単一 q ビットユニタリー変換を含む回路が与えられると，Hadamard，位相，制御 NOT および $\pi/8$ ゲートの離散的集合だけを使って，この回路を精度良くシミュレートできるという意味で，この Hadamard，位相，制御 NOT および $\pi/8$ ゲートは量子計算にとって普遍的ゲートである．さらにこのシミュレーションは効率的に実行できて，シミュレーションに必要な追加負担の倍数は $\log(m/\epsilon)$ の多項式に収まる．ここで $m$ は元の回路

のゲート数，$\epsilon$ はシミュレーションの要求精度である．

**演習 4.41:** これと次の 2 つの演習は，Hadamard，位相，制御 NOT および Toffoli ゲートが普遍的となる構成を明らかにする．図 4.17 の回路はもし測定結果が共に 0 ならば第 3 の（標的）q ビットに対して $R_z(\theta)$ を適用し，そうでなければ $Z$ を適用することを示せ．ここで $\cos\theta = 3/5$ である．両方の測定結果が 0 である確率は 5/8 であることを示し，この回路と $Z = S^2$ ゲートを繰り返し使うと，$R_z(\theta)$ ゲートの適用確率が 1 に近づくことを説明せよ．

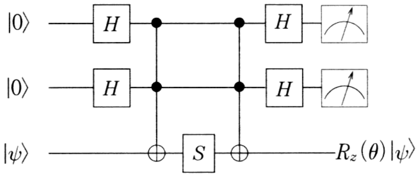



**図 4.17:** 両方の測定結果が 0 ならばこの回路は標的 q ビットに $R_z(\theta)$ を適用する．ここで $\cos\theta = 3/5$ である．もし測定結果がそれ以外ならば標的 q ビットに $Z$ を適用する．

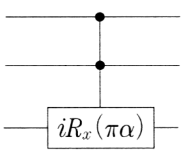
**演習 4.42:**（**無理数の** $\theta$）　$\cos\theta = 3/5$ とする．$\theta$ が $2\pi$ の無理数倍であることを背理法で証明する．

(1) $e^{i\theta} = (3+4i)/5$ を使って，もし $\theta$ が有理数ならば $(3+4i)^m = 5^m$ なる正の整数 $m$ が存在しなければならないことを示せ．

(2) すべての $m > 0$ に対して $(3+4i)^m = 3+4i \pmod 5$ を示し，$(3+4i)^m = 5^m$ なる $m$ は存在しないという結論を導け．

**演習 4.43:** 前の 2 つの演習の結果を使って Hadamard，位相，制御 NOT および Toffoli ゲートが量子計算の普遍的ゲートであることを示せ．

**演習 4.44:** 次の回路で定義される 3 - q ビットゲート $G$ は $\alpha$ が無理数のときにはいつでも量子計算に普遍的であることを示せ．



**演習 4.45:** $U$ はユニタリー演算であり，$H$, $S$, 制御 NOT および Toffoli ゲートで構成される $n$ 個の q ビット量子回路で実現されるとする．ある整数 $k$ に対して $U$ は $2^{-k/2}M$ の形をとることを示せ．ここで $M$ は複素整数の要素のみを持つ $2^n \times 2^n$ 行列である．Toffoli ゲートを $\pi/8$ ゲートで置き換えて同じことを示せ．

### 4.5.4　一般に困難な任意のユニタリーゲート近似

$n$ 個の q ビットに働く任意のユニタリー変換が少数の基本ゲートより成る集合で構築できることを見てきた．これは常に効率良くできるであろうか？ つまり $n$ 個の q ビットへのユニタリー変換 $U$ が与えられたとき，$U$ を近似する $n$ の多項式サイズの回路が常に存在するか？ この疑問に対する答えは no であることがわかっている．実際にたいていのユニタリー変換は非効率的にしか実行できない．これを理解するのに次の質問を考える：$n$ 個の q ビットの任意の状態を生成するには幾つのゲートが必要か？ 単純に数え上げると一般に指数関数的に多数の演算が必要になり，これから直ちに指数関数的数の演算を必要とするユニタリー演算があることが導ける．これを示すために $g$ 種類の異なるタイプのゲートがあり，各々のゲートがたかだか $f$ 個の入力 q ビットに作用するとする．この数 $f$ と $g$ は我々が使うコンピュータのハードウェアで決まっており，定数と考えられる．$m$ 個のゲートを含む量子回路があり，計算基底状態 $|0\rangle^{\otimes n}$ から出発するとしよう．したがって，回路中のどの特定のゲートに対しても，たかだか $\left[\begin{array}{c} n \\ f \end{array}\right]^g = O(n^{fg})$ 個の選択が可能である．この結果，$m$ 個のゲートを使ってたかだか $O(n^{fgm})$ 個の異なる状態を計算できる．

特定の状態 $|\psi\rangle$ を距離 $\epsilon$ 以内で近似するとする．証明の考え方はとり得るすべての状態の集合を半径 $\epsilon$ のパッチの集合でカバーし（図 4.18），必要なパッチの数が $n$ の 2 重指数関数で増加することを示す．$m$ 個のゲートを用いて計算し得る指数関数的数の異なる状態と比較すると結果がわかる．我々が最初に見るべきことは，$n$ 個の q ビットの状態ベクトル空間を，$(2^{n+1}-1)$ 次元単位球体と見なすことである．これを証明するために，$n$ - q ビット状態の振幅が $\psi_j = X_j + iY_j$ であるとする．ここで $X_j$ と $Y_j$ は $j$ 番目の振幅の実数部と虚数部である．量子状態の正規化

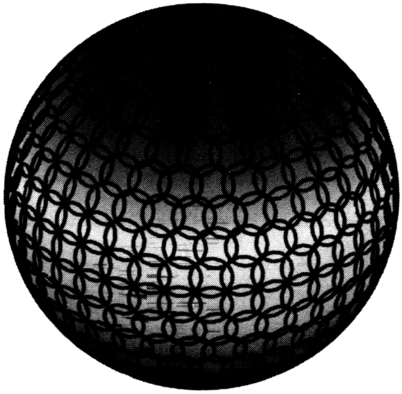


図 **4.18:** 一定半径のパッチで可能な状態の集合をカバーする様子.

条件は $\sum_j (X_j^2 + Y_j^2) = 1$ と書くことができ，これは点が $2^{n+1}$ 実次元の単位球表面上 — つまり $(2^{n+1}-1)$ 次元単位球体 — にある条件でもある．同様に $|\psi\rangle$ 近くの半径 $\epsilon$ の表面積は近似的に半径 $\epsilon$ の $(2^{n+1}-2)$ 次元球体の体積に等しい．半径 $r$ の $k$ 次元球体の表面積に対する式 $S_k(r) = 2\pi^{(k+1)/2}\ r^k/\Gamma((k+1)/2)$ と，半径 $r$ の $k$ 次元球体の体積に対する式 $V_k(r) = 2\pi^{(k+1)/2}\ r^{k+1}/[(k+1)\Gamma((k+1)/2)]$ を用いると，状態空間をカバーするパッチの数は次のようになる：

$$\frac{S_{2^{n+1}-1}(1)}{V_{2^{n+1}-2}(\epsilon)} = \frac{\sqrt{\pi}\Gamma(2^n - \frac{1}{2})(2^{n+1}-1)}{\Gamma(2^n)\epsilon^{2^{n+1}-1}}, \tag{4.82}$$

ここで $\Gamma$ は通常の一般的な階乗関数である．しかし $\Gamma(2^n - 1/2) \geq \Gamma(2^n)/2^n$ なので，空間をカバーするに要するパッチの数は少なくとも

$$\Omega\left(\frac{1}{\epsilon^{2^{n+1}-1}}\right). \tag{4.83}$$

$m$ 個のゲートでカバーできるパッチの数は $O(n^{fgm})$ であることを思い出すと，すべての $\epsilon$-パッチを実現するには

$$O(n^{fgm}) \geq \Omega\left(\frac{1}{\epsilon^{2^{n+1}-1}}\right). \tag{4.84}$$

これから

$$m = \Omega\Big(\frac{2^n \log(1/\epsilon)}{\log(n)}\Big). \tag{4.85}$$

つまり $\Omega(2^n \log(1/\epsilon)/\log(n))$ 個の演算により距離 $\epsilon$ 以内に近似できる，$n$ 個の q ビット状態が存在する．これは $n$ の指数関数であり，3 章（第 I 巻）で紹介した計算量の意味で「困難」である．さらにこれからただちに，誤差 $E(U, V) \le \epsilon$ となるように演算 $V$ を実行する量子回路を用いると，$n$ 個の q ビットに作用するユニタリー変換 $U$ を $\Omega(2^n \log(1/\epsilon)/\log(n))$ 回の演算で近似できことがわかる．これに対して我々の普遍的構成と Solovay-Kitaev の定理を用いると，$n$ 個の q ビットに働く任意のユニタリー演算 $U$ は，$\epsilon$ 以下の距離で $O(n^2 4^n \log^c(n^2 4^n/\epsilon))$ 個のゲートで近似し得る．したがって，我々が与えた普遍的構成は多項式因子の範囲内で最適なものである．残念ながら量子回路モデルでどのような族 (family) のユニタリー演算が計算できるかを決める問題はこれでは扱えない．

### 4.5.5　量子計算量

3 章（第 I 巻）において，古典コンピュータ上の計算問題を解くのに必要なリソース要求を分類するための，「計算量」理論について述べた．当然ながら量子計算量の理論を発展させ古典計算量理論との関連を明らかにしようという関心が高まっている．まだこの方向に踏み出したばかりであるが，将来の研究者にとって非常に実り多い方向であるのは疑いない．ここでは量子計算量クラス **BQP** と古典計算量クラス **PSPACE** の関係を示す，量子計算量に関する 1 つの結果を紹介するにとどめる．この結果に関する議論はあまり形式ばらないものであり，詳しい結果は章末の「歴史と参考資料」で述べる Bernstein と Vazirani の論文を見て欲しい．

3 章（第 I 巻）において，**PSPACE** は問題のサイズ内で多項式量の空間と任意の時間を使って，Turung 機械上で解くことができる決定問題であると定義したことを思い出そう．**BQP** は多項式サイズの量子回路を用いて，有界の誤り確率で解ける決定問題よりなる量子計算量クラスである．少し形式的に言えば言語中に含まれる記号列を少なくとも 3/4 の確率で受け入れ，その言語にない記号列を少なくとも 3/4 の確率で排除するような言語を決定する多項式サイズの量子回路族が存在するとき，その言語 $L$ は **BQP** にあるという．実際にこれが意味するところは量子回路に 2 進数記号列を入力し，それが言語中の要素であるかどうかを決定することである．この回路出力では 1 個の q ビットを測定して，結果が 0 な

らば記号列は受理され1ならば拒絶される．記号列が $L$ にあるかどうかのテストを数回行うと，与えられた記号列が $L$ にあるかどうかが高確率で決定できる．

もちろん量子回路は固定しており，どんな量子回路が与えられてもある有限長の記号列までが $L$ にあるかどうかが決定できるだけである．この理由で **BQP** の定義にはすべての回路族 (family of circuits) を使う．可能な入力長毎に異なる回路が回路族中に存在するからである．すでに述べた受理または拒否の判断基準に加えて，回路にもう2つの制約を加える．第1は回路サイズが，言語 $L$ 中の存在を判断しようとしている入力記号列 $x$ のサイズと共に，多項式数でしか増大しないことである．第2の要求は3.1.2項（第I巻）で述べたのと同じ意味で，回路が**一様に生成**されることである．この一様性の要請は次の理由で生じる．実際にある長さ $n$ の記号列 $x$ が与えられると，誰かが $x$ が $L$ にあるかどうかを決めることができる量子回路を構築しなければならないからである．これを行うには回路構築のための明瞭な指令セット — アルゴリズム — を必要とする．これには量子回路が一様に生成されたものであること — つまり量子回路の記述を効率良く出力することができる Turing 機械が存在すること — が要求される．この制約はテクニカルなものに見えるかも知れないし，実際問題としてほとんど常に満たされるものであるが，3.1.2項（第I巻）で述べた異常な事態に陥ることを防いでくれる．(一様性の要請に使われる Turing 機械が量子的なものか古典的なものかという問題を懸念するかも知れないが，それは重要でないことがわかっている — 「歴史と参考資料」欄参照.）

量子計算量理論における最も重要な結果の1つは $\mathbf{BQP} \subseteq \mathbf{PSPACE}$ である．古典的 Turing 機械上で多項式時間を使って，有界誤り確率で解ける決定問題の古典計算量クラスを **BPP** とすると，$\mathbf{BPP} \subseteq \mathbf{BQP}$ であることは明らかである．したがって，$\mathbf{BPP} \subseteq \mathbf{BQP} \subseteq \mathbf{PSPACE}$ という一連の内包関係が得られる．$\mathbf{BQP} \neq \mathbf{BPP}$ — 直観的には量子コンピュータは古典コンピュータより強力だということ — を証明すると，それは $\mathbf{BPP} \neq \mathbf{PSPACE}$ であることを意味する．しかし現在のところ $\mathbf{BPP} \neq \mathbf{PSPACE}$ かどうかわかっておらず，これが証明されれば古典コンピュータ科学の大きな突破口となろう！ 量子コンピュータが古典コンピュータより強力であることを証明すると，古典計算量に対しても非常に興味深くかつ意義がある！ 残念ながらそれは証明が極めて困難であることも意味している．

**BQP** $\subseteq$ **PSPACE** であるのはなぜか？ 証明の概略を直観的に示すとこうなる（厳密な証明は「歴史と参考資料」参照）．q ビット数が $n$ の量子コンピュータがあり，一連のゲートを $p(n)$ 個含む計算を行うとする．ここで $p(n)$ は $n$ の多項式である．量子回路の初期状態を $|\psi\rangle$ とし，その終状態が $|y\rangle$ となる確率を古典コンピュータ上の多項式空間で評価する方法を説明する．量子コンピュータ上で実行されるゲートが $U_1$，$U_2, \ldots, U_{p(n)}$ の順であるとする．このとき，状態 $|y\rangle$ で終わる確率は

$$\langle y|U_{p(n)} \cdots U_2 U_1|0\rangle \tag{4.86}$$

の絶対値の 2 乗である．この量は古典コンピュータ上の多項式空間で推定できる．基本的考え方は式 (4.86) の各因子間に完全性関係式 $\sum_x |x\rangle\langle x| = I$ を挿入すると：

$$\begin{aligned}&\langle y|U_{p(n)} \cdots U_2 U_1|0\rangle &(4.87)\\ &= \sum_{x_1,\ldots,x_{p(n)-1}} \langle y|U_{p(n)}|x_{p(n)-1}\rangle\langle x_{p(n)-1}|U_{p(n)-1} \ldots U_2|x_1\rangle\langle x_1|U_1|0\rangle.\end{aligned}$$

総和に現れる各ユニタリーゲートが Hadamard ゲート，制御 NOT 等々のオペレータであることが与えられると，総和中の各項は古典コンピュータ上の多項式空間だけを使って高精度で計算できて，したがって総和の各項は和をとると消えるので，総和全体が多項式空間を使って計算できるのは明らかである．もちろん計算で和をとるべき総和中の項数が指数関数的多数にのぼるので，このアルゴリズムは早くない．しかし多項式空間を使うだけなので，最初に示したように **BQP** $\subseteq$ **PSPACE** である．

同様な手順で**任意の**量子計算をその長さに関係なく，古典コンピュータ上でシミュレートすることができる．したがって，無制限の時間と空間リソースを使って量子コンピュータ上で解ける問題のクラスは，古典コンピュータ上で解ける問題のクラスより大きくない．換言すればこの意味は，量子コンピュータが「任意のアルゴリズムは，Turing 機械を用いてシミュレートできる」とする Church-Turing の提唱に反するものではない．もちろん量子コンピュータは古典コンピュータに比べてはるかに**効率良く**なり得るので，任意のアルゴリズムは確率的 Turing 機械を使って**効率良く**シミュレートできるとする，**強い**Church-Turing の提唱に挑戦することになる．

## 4.6　計算の量子回路モデルのまとめ

本書で「量子コンピュータ」とは計算の量子回路モデルと同義である．本章では量子回路，その基本要素，普遍的ゲート族，および幾つかの応用について詳しく述べた．もっと複雑な応用に移る前に計算の量子回路モデルの鍵となる事項をまとめておく：

(1) **古典的リソース：** 量子コンピュータは古典的部分と量子的部分の 2 つの部分より成る．原理上古典的部分は必要ないが，実際上は一部を古典的に実行するほうがある種のタスクを容易に行える．例えば量子誤り訂正（10 章：第 III 巻）の多くの方法に，効率を最大にするための古典計算が含まれている．古典計算は原理上常に量子コンピュータで行えるが，古典コンピュータ上で計算するのが便利なことがある．

(2) **適合する状態空間：** 量子回路はある数 $n$ の q ビットに作用する．したがって状態空間は $2^n$ 次元の複素 Hilbert 空間である．$|x_1, \ldots, x_n\rangle$ の形の積状態をコンピュータの**計算基底状態**と呼ぶ．ここで，$x_i = 0,\ 1$ である．$|x\rangle$ は計算基底状態を表す．ここで数 $x$ の 2 進数表現が $x_1 \ldots x_n$ である．

(3) **計算基底状態を準備する能力：** 任意の計算基底状態 $|x_1, \ldots, x_n\rangle$ はたかだか $n$ ステップで準備できると仮定する．

(4) **量子ゲートを実行する能力：** q ビットの任意の部分集合に望み通りのゲートを適用できて，普遍的ゲート族が実現できる．例えば，量子コンピュータで任意の q ビット対に対して制御 NOT ゲートが適用できなければならない．Hadamard，位相，制御 NOT および $\pi/8$ ゲートは任意のユニタリー演算を近似できるゲート族を形成するので，普遍的ゲートの集合である．他にも普遍的集合は存在する．

(5) **計算基底で測定する能力：** コンピュータ中の 1 つあるいはそれ以上の q ビットの計算基底において測定を実行することができる．

量子計算の量子回路モデルは，同じ問題に対して本質的に同じリソースを必要とするという意味で，これまでに提案された他の多くの計算モデルと等価である．基本概念を示す簡単な例をあげると，2 準位の q ビットに代わって 3 準位の量子システムを基本として設計すると，計算上の利点が生まれると思うかも知れない．

もちろん 3 準位量子システム（**q** トリット (qutrit)）を用いると，2 準位に比べて僅かに利点があるが，理論的見地からその差は本質的に無視できる．もう少し意味のある話に目を向けると，古典 Turing 機械モデルの量子版すなわち計算の「量子 Turing 機械」モデルが，量子回路に基づくモデルと等価であることが示されている．本書ではこのモデルは考えなかったが，量子 Turing 機械の勉強に興味を持つ読者には，章末の「歴史と参考資料」にある文献を調べることを勧める．

量子回路モデルは簡単で魅力的であるが，それに対する批判，修正および拡張について心に留めておくとよい．例えば，量子回路モデルの状態空間や初期条件に関する基本的仮定が正当化されているかどうかは全く明らかでない．すべてが有限次元の状態空間で表現されているが，無限次元の状態空間を有するシステムを使うと何か利益があるか？ コンピュータの初期状態が計算基底状態であるという仮定も必要でない．自然界の多くのシステムが多数システムの高度なもつれ状態になるのを「好む」ことを我々は知っている．この選択を利用して計算能力をさらに強めることはできないか？ 計算基底から出発する制約よりは，別の状態を利用したほうが特定の計算が容易になるかも知れない．同様に多 q ビット基底でもつれ測定を効率良く行う能力があれば，もつれを起こすユニタリー演算を実行できるのと同じくらい有用であろう．実際そのような測定を利用して，量子回路モデルだけでは手に負えないタスクを実行することが可能になるかも知れない．

量子回路モデルの底に潜む，物理学の詳細な検証や正当化の試みは本書の議論の範囲外であり，実際のところ現在の知識をも越えている！ これらの事項を列挙することによって量子回路モデルの完全性に対する疑問を紹介し，情報は物理的であるという基本点を再び強調しておきたい．情報処理モデルを確立する試みの中で，我々は常に基本的物理学法則に立ち返るべきである．本書の目的のために我々は計算の量子回路モデルの範囲内に留まる．それにより量子力学の性質を利用した豊富で強力な計算モデルを提供して，古典的前例のない情報処理の素晴らしい偉業が達成できる．量子回路モデルを越える物理的に合理的な計算モデルが存在するかどうかは，読者に託される未解決の問題である．

## 4.7 量子システムのシミュレーション

> 多分 ... 我々には量子オートマトンの数学的理論が必要である. ... 量子状態空間は古典的空間よりはるかに大きな容量を持っている: 古典的システムが $N$ 状態を有するのに対して重ね合せを許容するその量子版では $c^N$ 状態を収容する. 2 つの古典的システムを結合するとその状態数は $N_1$ と $N_2$ の積になる. 一方量子の場合には $c^{N_1 N_2}$ と指数関数的に増加する. ... この粗い推定でもシステムの量子的振る舞いは, その古典的シミュレーションよりはるかに複雑であることを示している. — Yu Manin(1980)[Man80], 翻訳は [Man99]

> メタン分子 1 個を量子力学的に計算するには $10^{42}$ 個のグリッド点が必要になる. 各点で僅か 10 回の基本演算を行い, しかも超極低温 $T = 3 \times 10^{-3}$K で計算すると仮定しても, 過去 1 世紀間に地上で生産されたエネルギーをすべて消費することになる.
> — R. P. Poplavskii (1975)[Pop75], Manin による引用

> 普遍的コンピュータで物理学をシミュレーションできるか? ... 物理的世界は量子力学的なので, したがって適切な設問は量子力学のシミュレーションができるか?である ... $R$ 個の粒子を持つ大きなシステムに対する完全な量子力学的記述は ... あまりに変数が多いので, $R$ に比例する要素数の通常のコンピュータでは**シミュレーションできない** ... しかし量子コンピュータの要素を使えば可能である. 古典的な (敢えて確率的と仮定する) 普遍的コンピュータを使って量子システムを確率的にシミュレーションできるか? ... もしこれまで述べた種類の古典コンピュータを使ってならば ... 答えは確実に No! である. — Richard P. Feynman (1982) [Fey82]

本章の最後に量子回路モデルの興味深く有益な応用を紹介する. 計算の最も重要な具体的応用の 1 つは物理システムのシミュレーションである. 例えば新しい建物の技術的設計において, 有限要素解析とモデル化がコスト最小化と安全性確保のために使われる. コンピュータ支援設計 (CAD) を用いて軽量, 安全構造, 魅力的, 低価格の車が作られる. 近代的航空工学は飛行体の設計において, 流体力

学のコンピュータシミュレーションに深く依存している．核兵器はもはや爆発されることは（たいていの場合は）なく，大規模な計算モデルによりテストされる．予言的シミュレーションは素晴らしい実用的応用の可能性を持つので，その実例は豊富にある．最初に幾つかのシミュレーション問題の事例を示し，次にシミュレーションの量子アルゴリズムと実例，最後にその応用展望について述べる．

### 4.7.1　シミュレーションの実行

シミュレーションの中心課題は，システムのダイナミックな振る舞いを規定する物理学法則を捉える，微分方程式を解くことである．ある例ではそれがNewtonの法則であり：

$$\frac{d}{dt}\left(m\frac{dx}{dt}\right) = F, \tag{4.88}$$

Poissonの方程式であり：

$$-\vec{\nabla}\cdot(k\vec{\nabla}\vec{u}) = \vec{Q}, \tag{4.89}$$

電磁気ベクトルの波動方程式であり：

$$\vec{\nabla}\cdot\vec{\nabla}\vec{E} = \epsilon_0\mu_0\frac{\partial^2\vec{E}}{\partial t^2}, \tag{4.90}$$

拡散方程式であり：

$$\vec{\nabla}^2\psi = \frac{1}{a^2}\frac{\partial\psi}{\partial t}, \tag{4.91}$$

これらはほんの一例に過ぎない．一般にゴールはシステムの最初の状態が与えられたとき，他の時間および/または位置における状態は何か？である．通常状態をディジタル表現で**近似**し，次に手続きを繰り返すことにより状態が始状態から終状態に進むように，微分方程式を空間と時間で**離散化**して解を得る．重要なことはこの手続きの誤差が有界であり，少ない繰り返し回数のベキ乗より早くは増大しないことがわかっている点である．さらにすべての動的システムが**効率良く**近似されるわけではない．一般に効率良く記述できるシステムだけが効率良くシミュレートできる．

古典コンピュータによる量子システムのシミュレーションは可能であるが，しかし一般に極めて効率が悪い．多くの単純な量子システムの動的振る舞いは

Schrödinger の方程式で支配される：

$$i\hbar\frac{d}{dt}|\psi\rangle = H|\psi\rangle. \tag{4.92}$$

$\hbar$ を $H$ の中に吸収するのが便利であり，本書でもこの慣習を踏襲する．（これまで扱ってきた q ビットのような抽象的システムでなく！）空間中の実際の粒子を扱う物理学者が関心を持つ典型的 Hamiltonian に対して，この式は位置表現と呼ぶ慣用表記 $\langle x|\psi\rangle = \psi(x)$ を用いて

$$i\frac{\partial}{\partial t}\psi(x) = \left[-\frac{1}{2m}\frac{\partial^2}{\partial x^2} + V(x)\right]\psi(x) \tag{4.93}$$

と表される．これは式 (4.91) によく似た楕円方程式である．したがって，Schrödinger 方程式は量子システムのシミュレーションが直面する特別困難な問題というわけではない．何が困難なのか？

量子システムをシミュレートする際の主要な困難さは，解くべき微分方程式の数が**指数関数的**であることにある．Schrödonger 方程式に従って時間発展する 1 つの q ビットに対して，2 つの微分方程式系を解かねばならない．2 つの q ビットでは 4 つの方程式，$n$ 個の q ビットでは $2^n$ 個の方程式である．時には洞察力に満ちた近似により関連する方程式の実効的数を減らすことができれば，量子システムの古典的シミュレーションが可能になる．しかしそのような近似が知られていなくて物理的に興味深い量子システムは数多い．

**演習 4.46:（量子システムの指数関数的複雑性の増大）** $\rho$ は $n$ 個の q ビットの状態を記述する密度行列である．$\rho$ を記述するには $4^n - 1$ 個の独立な実数が必要となることを示せ．

物理学の素養を持つ読者は古典的シミュレーションには手に負えない多くの重要な量子システムがあることの重要性を認識するかも知れない．この中には Hamiltonian：

$$H = \sum_{k=1}^{n} V_0 n_{k\uparrow} n_{k\downarrow} + \sum_{k,\ j\ \text{近傍},\ \sigma} t_0 c^*_{k\sigma} c_{j\sigma}, \tag{4.94}$$

を有し，超伝導や磁性の研究で重要な相互作用するフェルミオン粒子のモデルである Hubbard モデルや，Ising モデル：

$$H = \sum_{k=1}^{n} \vec{\sigma}_k \cdot \vec{\sigma}_{k+1}, \tag{4.95}$$

その他多数がある．このようなモデルの解によって材料の誘電率，伝導率，透磁率など多くの物理的性質が得られる．もう少し複雑な量子電気力学（QED; quantum electrodynamics）や量子クロモ力学（QCD; quantum chromodynamics）を用いると陽子の質量のような物理定数が計算できる．

量子コンピュータは，効率的な古典的シミュレーションが知られていない量子システムを，効率的にシミュレートできる．これが可能なのは，直観的に量子ゲートの普遍的集合から任意の量子回路が構築できるのと全く同じ理由である．さらに**効率良く**近似できないユニタリー演算が存在するように，量子コンピュータによって効率良くシミュレートできない Hamiltonian を持つ，量子システムを想像することは原理上可能である．もちろん，もしそのような量子システムが存在すれば，それを使って量子回路モデルを越す情報処理が可能になるので，そのようなシステムは自然界に実現し得ないと信じているが．

### 4.7.2　量子シミュレーションアルゴリズム

古典的シミュレーションは $dy/dt = f(y)$ のような簡単な微分方程式を解くに際して，1 次の範囲で $y(t+\Delta t) \approx y(t) + f(y)\Delta t$ が成り立つと認識するところからはじまる．同様に量子的シミュレーションでは $i\ d|\psi\rangle/dt = H|\psi\rangle$ を解く．その解は $H$ が時間に依存しない場合に次式で与えられる：

$$|\psi(t)\rangle = e^{-iHt}|\psi(0)\rangle. \tag{4.96}$$

通常 $H$ を指数関数化することは非常に難しい（$H$ を表す行列は散発的かも知れないが指数関数的に大きい）ので，最初は 1 次解 $|\psi(t+\Delta t)\rangle \approx (I - iH\Delta t)|\psi(t)\rangle$ から出発するのがよい．多くの Hamiltonian　$H$ に対して $I - iH\Delta t$ を効率良く近似する量子ゲートを直接構成できるので，これは扱うことができる．しかしそのような 1 次解は一般に満足できるものではない．

多くのクラスの Hamiltonian に対して式 (4.96) の高次の効率的近似解が可能である．例えば，たいていの物理システムの Hamiltonian は多くの局所的相互作

用の和として書ける．特に $n$ 個の粒子のシステムに対して

$$H = \sum_{k=1}^{L} H_k, \tag{4.97}$$

ここで各 $H_k$ はたかだか定数 $c$ 個のシステムに作用し，$L$ は $n$ の多項式である．例えば，項 $H_k$ はしばしば $X_iX_j$ のような 2 体相互作用と，$X_i$ のような単体 Hamiltonian を表す．Hubbard モデルと Ising モデルはこの形の Hamiltonian を有している．このような局所性には物理的な合理性があり，多くのシステムにおけるたいていの相互作用は距離やエネルギー差が増すに従って相互作用が減少することに起因している．時には粒子統計のように付加的な全体的対称性の制約が生じる場合があり，まもなくこの例に出会う．重要なのは $e^{-iHt}$ を計算するのは難しいが，$e^{-iH_kt}$ ははるかに少数の部分システムに働くので，量子回路を用いて直接近似できる点である．しかし一般に $[H_j, H_k] \neq 0$ なので，$e^{-iHt} \neq \prod_k e^{-iH_kt}$ である！ とすれば如何にして $e^{-iH_kt}$ を用いて $e^{-iHt}$ を構成するか？

**演習 4.47:** $H = \sum_k^L H_k$ に対してすべての $j, k$ で $[H_j, H_k] = 0$ ならば，すべての $t$ に対して $e^{-iHt} = e^{-iH_1t}\, e^{-iH_2t} \ldots e^{-iH_Lt}$ であることを証明せよ．

**演習 4.48:** $H_k$ がたかだか $c$ 個の粒子を含むための制約は，式 (4.97) の総和において $L$ が $n$ の多項式により上に有界であることを**意味する**のを証明せよ．

量子シミュレーションアルゴリズムの核心は次の漸近近似定理である：

**定理 4.3:（Trotter の公式）** $A$ と $B$ が Hermite オペレータとすると，任意の実数 $t$ に対して

$$\lim_{n\to\infty} \left(e^{iAt/n} e^{iBt/n}\right)^n = e^{i(A+B)t}. \tag{4.98}$$

式 (4.98) は $A$ と $B$ が可換でなくても成立することに注意する．多分もっと興味深いのは，一般的量子オペレータに対応するある種の半群 (semigroup) の生成元 (generator) である $A$ と $B$ に対しても，成り立つように一般化できる．そのような生成元（「Lindblad 形式」）については 8.4.1 項（第 III 巻）で述べる．ここでは $A$ と $B$ が Hermite 行列である場合だけを考える．

**証明**　定義により

$$e^{iAt/n} = I + \frac{1}{n}iAt + O\left(\frac{1}{n^2}\right), \tag{4.99}$$

したがって

$$e^{iAt/n}e^{iBt/n} = I + \frac{1}{n}i(A+B)t + O\left(\frac{1}{n^2}\right). \tag{4.100}$$

式 (4.100) より

$$e^{iAt/n}e^{iBt/n} = e^{i(A+B)t/n} + O\left(\frac{1}{n^2}\right). \tag{4.101}$$

$n$ 乗をとると

$$\left(e^{iAt/n}e^{iBt/n}\right)^n = e^{i(A+B)t} + O\left(\frac{1}{n}\right). \tag{4.102}$$

この式より結論の式 (4.98) が得られる．ベキ乗による誤差項の変化にはコラム 4.1 の式 (4.69) のような不等式を用いる必要がある．　□

Trotter の公式を変形すると，量子シミュレーションを行うための高次近似を導く方法が得られる．例えば上の証明と同様の筋道で次式が示せる．

$$e^{i(A+B)\Delta t} = e^{iA\Delta t}e^{iB\Delta t} + O(\Delta t^2). \tag{4.103}$$

同様に

$$e^{i(A+B)\Delta t} = e^{iA\Delta t/2}e^{iB\Delta t}e^{iA\Delta t/2} + O(\Delta t^3). \tag{4.104}$$

量子シミュレーションアルゴリズムのまとめを下に示す．また 1 次元非相対論的 Schrödinger 方程式の明示的シミュレーションをコラム 4.2 に示す．

**アルゴリズム： 量子シミュレーション**

**入力：** (1) $N$ 次元システムに作用する Hamiltonian $H = \sum_k H_k$，ただし各 $H_k$ は $N$ に無関係なサイズの小さな部分システムに作用する．

(2) $t = 0$ におけるシステムの初期状態 $|\psi_0\rangle$ .

(3) 正で 0 でない精度 $\delta$ .

(4) 時間発展して所望の状態になる時刻 $t_f$ .

**出力：** $|\langle\tilde{\psi}(t_f)|e^{-iHt_f}|\psi_0\rangle|^2 \geq 1-\delta$ なる状態 $|\tilde{\psi}(t_f)\rangle$ .

**演算回数：** $O(\mathrm{poly}(1/\delta))$ 回の演算.

**手続き：** $n = \mathrm{poly}(\log N)$ 個の q ビットの状態 $|\tilde{\psi}\rangle$ がシステムを近似し，オペレータ $e^{-iH_k\Delta t}$ が効率の良い量子回路近似となるような表現を選ぶ．近似方法（例えば，式 (4.103)～(4.105) 参照）と，予想される誤差が許容できる（整数 $j$ に対して $j\Delta t = t_f$ となる）ように $\Delta t$ を選択し，反復ステップに対する量子回路 $U_{\Delta t}$ を構築して次のステップを実行する：

| | | |
|---|---|---|
| **1**. | $|\tilde{\psi}_0\rangle \leftarrow |\psi_0\rangle;\ j=0$ | 状態初期化 |
| **2**. | $\rightarrow |\tilde{\psi}_{j+1}\rangle = U_{\Delta t}|\tilde{\psi}_j\rangle$ | 反復更新 |
| **3**. | $\rightarrow j = j+1;\ \ j\Delta t \geq t_f$ となるまで **2** に戻る | ループ実行 |
| **4**. | $\rightarrow |\tilde{\psi}(t_f)\rangle = |\tilde{\psi}_j\rangle$ | 最終結果 |

**演習 4.49:（Baker-Campbell-Hausdorf の公式）** 次式と式 (4.103), (4.104) を証明せよ．

$$e^{(A+B)\Delta t} = e^{A\Delta t}e^{B\Delta t}e^{-\frac{1}{2}[A,\ B]\Delta t^2} + O(\Delta t^3). \tag{4.105}$$

**演習 4.50:** $H = \sum_k^L H_k$ として次式を定義する．

$$\begin{aligned} U_{\Delta t} = &\left[e^{-iH_1\Delta t}e^{-iH_2\Delta t}\dots e^{-iH_L\Delta t}\right] \\ &\left[e^{-iH_L\Delta t}e^{-iH_{L-1}\Delta t}\dots e^{-iH_1\Delta t}\right]. \end{aligned} \tag{4.106}$$

(1) $U_{\Delta t} = e^{-2iH\Delta t} + O(\Delta t^3)$ を証明せよ．

(2) コラム 4.1 の結果を用いて正の整数 $m$ とある定数 $\alpha$ に対して次式を証明せよ．

$$E(U_{\Delta t}^m, e^{-2miH\Delta t}) \leq m\alpha\Delta t^3. \tag{4.107}$$

**コラム 4.2: Schrödinger の方程式の量子シミュレーション**

量子シミュレーションの方法と限界について抽象的 q ビットモデルより，物理学者が研究した伝統的方法による次の例のほうが，うまく説明できるかも知

れない．1 次元ポテンシャル $V$ 内の線上を動く単一粒子が次の Hamiltonian に従うとする．

$$H = \frac{p^2}{2m} + V(x), \tag{4.108}$$

ここで $p$ は運動量オペレータ，$x$ は位置オペレータである．$x$ の固有値は連続であり，システムの状態 $|\psi\rangle$ は無限次元の Hilbert 空間に存在する．$x$ 基底において状態は次のように書ける．

$$|\psi\rangle = \int_{-\infty}^{\infty} |x\rangle\langle x|\psi\rangle dx. \tag{4.109}$$

実際上興味を持つのはある有限領域であり，領域 $-d \le x \le d$ としてよい．さらに

$$|\tilde{\psi}\rangle = \sum_{k=-d/\Delta x}^{d/\Delta x} a_k |k\Delta x\rangle \tag{4.110}$$

が $|\psi\rangle$ の良い物理的近似になるように，微分ステップの大きさ $\Delta x$ をシステムの最短波長に比べて十分小さく選ぶことができる．この状態は $n = \lceil \log(2d/\Delta x + 1) \rceil$ 個の q ビットを用いて表現できる．単純に基底 $|k\Delta x\rangle$（オペレータ $x$ の固有状態）を $n$ 個の q ビットの計算基底状態である $|k\rangle$ で置き換える．このシミュレーションでは $n$ 個の q ビットしか要らないのに対して，古典的には $2^n$ 個の複素数を追跡せねばならず，量子コンピュータシミュレーションにより指数関数的リソースの節約になる．

$|\tilde{\psi}(t)\rangle = e^{-iHt}|\tilde{\psi}(0)\rangle$ の計算には，一般に $H_1 = V(x)$ が $H_0 = p^2/2m$ と可換でないので，近似 (4.103)～(4.105) を使う必要がある．したがって $e^{-iH_1\Delta t}$ と $e^{-iH_0\Delta t}$ が計算できなければならない．$|\tilde{\psi}\rangle$ が $H_1$ の固有基底で表現されるので， $e^{-iH_1\Delta t}$ は次の形の対角変換となる．

$$|k\rangle \to e^{-iV(k\Delta x)\Delta t}|k\rangle. \tag{4.111}$$

$V(k\Delta x)\Delta t$ が計算できるので上式はただちに計算できる（問題 4.1 も参照）．第 2 因子も簡単である．なぜなら $x$ と $p$ は量子 Fourier 変換 $U_{\rm FFT} x U_{\rm FFT}^\dagger = p$ に関係した共役変数であり，したがって $e^{-iH_0\Delta t} = U_{\rm FFT} e^{-ix^2\Delta t/2m} U_{\rm FFT}^\dagger$

である．$e^{-iH_0\Delta t}$ の計算には

$$|k\rangle \to U_{\mathrm{FFT}} e^{-ix^2/2m} U_{\mathrm{FFT}}^{\dagger} |k\rangle \tag{4.112}$$

を実行する．$U_{\mathrm{FFT}}$ の構築については5章で議論する．

### 4.7.3 実 例

量子シミュレーションに関してこれまで述べてきた手続きは，局所的相互作用の総和であるHamiltonianのシミュレーションを中心としてきた．しかしこれは基本的要請ではない！ 次の例が示すように，大きなシステム全体あるいはほぼ全体に有意に働くHamiltonianに対しても，効率良い量子シミュレーションが可能である．

$n$ 個のqビットシステムに働く次のHamiltonianを考える：

$$H = Z_1 \otimes Z_2 \otimes \cdots \otimes Z_n. \tag{4.113}$$

これはシステム全体の相互作用を含んでいるにもかかわらず，実際に効率良くシミュレートできる．我々の目的は任意の $\Delta t$ 値に対して $e^{-iH\Delta t}$ を実行する簡単な量子回路である．$n=3$ に対してこれを正確に行う回路を図4.19に示す．主な着眼点はHamiltonianがシステムの全qビットを含んでいるが，それは**古典的な方法**によるのである．つまり，もし計算基底における $n$ 個のqビットの**パリティ** (parity) が偶数ならばシステムに与えられる位相は $e^{-i\Delta t}$ であり，そうでなければ $e^{i\Delta t}$ である．したがって，最初にパリティを古典的に計算し（結果を補助qビットに蓄積し），次にパリティの条件に応じて適切な位相シフトを適用し，次に（補助qビットを消去するために）パリティの逆計算を行う．明らかにこの戦略は $n=3$ のときだけでなく任意の $n$ に対して成り立つ．

同じ手続きをさらに発展させると，もっと複雑で拡大したHamiltonianをシミュレートできる．特に次の形の任意のHamiltonianを効率良くシミュレートできる：

$$H = \bigotimes_{k=1}^{n} \sigma_{c(k)}^{k}, \tag{4.114}$$

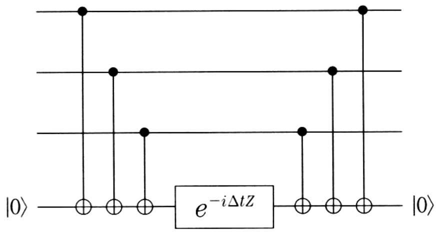



**図 4.19:** 時間 $\Delta t$ に対する Hamiltonian $H = Z_1 \otimes Z_2 \otimes Z_3$ をシミュレートする量子回路.

ここで $\sigma^k_{c(k)}$ は $k$ 番目の q ビットに働く Pauli の行列（または単位行列）であり，$c(k) \in \{0, 1, 2, 3\}$ は $\{I, X, Y, Z\}$ の 1 つを指定する．単位行列を実行する q ビットは無視してよく，$X$ と $Y$ の項は単一 q ビットゲートで $Z$ 演算に変換される．後に残るのは式 (4.113) の形の Hamiltonian であり，上述のようにシミュレートできる．

**演習 4.51:** 任意の $\Delta t$ に対してユニタリー変換 $e^{-i\Delta tH}$ を実行する Hamiltonian：

$$H = X_1 \otimes Y_2 \otimes Z_3 \tag{4.115}$$

をシミュレートする量子回路を構築せよ．

この手続きを使うと，局所的でない項を含む広範囲の Hamiltonian をシミュレートできる．特に $H = \sum_{k=1}^{L} H_k$ の形の Hamiltonian をシミュレートできる．ここで各 $H_k$ はテンソル積構造を持つことと，$L$ は全粒子数 $n$ の多項式であることが唯一の制約である．一般に唯一の条件は各 $H_k$ を別々にシミュレートする効率良い回路が存在することである．例えば Hamiltonian $H = \sum_{k=1}^{n} X_k + Z^{\otimes n}$ は上のテクニックを使って容易にシミュレートできる．このような Hamiltonian は概して自然界に生じないが，量子アルゴリズムの世界に新しく多分価値ある展望をもたらす．

### 4.7.4　量子シミュレーションの展望

量子シミュレーションアルゴリズムは古典的方法と非常に似ているが，同時に基本的に異なるところもある．量子アルゴリズムでは繰り返すたびに，古い状態

を新しい状態に置き換えなければならない．状態が量子的なのでアルゴリズムを変更しなければ，中間ステップで（意味のある）情報を得ることができない．さらに最終的測定は量子状態を乱すので，希望する結果が得られるように巧妙に選択しなければならない．もちろん量子シミュレーションを繰り返すと統計が得られるが，アルゴリズムを繰り返す回数はたかだか多項式回であるのが望ましい．シミュレーションを効率的に実行できるとしても，希望する測定を効率良く実行できないこともあり得る．

簡単にシミュレートできない Hamiltonian も存在する．4.5.4 項で量子コンピュータが効率良く近似できないユニタリー変換が存在することを知った．必然的にすべての Hamiltonian の時間発展が量子コンピュータ上で効率良くシミュレートできるとは限らない．なぜならもしできるとすれば，全ユニタリー変換が効率良く近似できることになるからである！

もう 1 つの困難な問題は — 興味ある問題でもあるが — 平衡化過程のシミュレーションである．温度 $T$ の環境と接する Hamiltonian $H$ で表されるシステムは一般に **Gibbs の状態** (Gibbs state) と呼ぶ熱平衡状態 $\rho_{\text{therm}} = e^{-H/k_{\text{B}}T}/\mathcal{Z}$ に達する．ここで $k_{\text{B}}$ は Boltzmann の定数，$\mathcal{Z} = \text{tr}\ e^{-H/k_{\text{B}}T}$ は正規化のための通常の分配関数であり $\text{tr}\ (\rho) = 1$ を保証する．この平衡化が進む過程は十分理解されていないが，ある種の必要条件ならばわかっている：環境が十分に大きく $H$ の固有状態に対応するエネルギー状態の分布が 0 でないことと，システムと環境の結合が弱いことである．任意の $H$ と $T$ に対する $\rho_{\text{therm}}$ を求めるのは，一般に古典コンピュータにおいて指数関数的に困難な問題である．量子コンピュータができれば効率良く解けるか？ それはまだわからない．

他方でここで示した単純なアルゴリズム以上に別の制約を有する場合でも，上で議論したように，実際に量子コンピュータを用いて多くの興味ある量子問題を効率的にシミュレートできる．これらの特別なクラスには粒子統計に基づくグローバルな対称性問題がある．日常世界で我々は異なる粒子を区別できることに慣れている．テニスコートではテニスボールを追いかけたり，飛跡をたどることができる．この飛跡がたどれることは古典的対象物の一般的特徴であり，古典的粒子の位置を連続に測定して，常に見失わないよう一意に他から見分けることができる．しかしこれは量子力学では破綻し，各粒子の運動を正確にたどることができない．もし 2 つの粒子が — 例えば陽子と電子のように — 本来異なるものなら

ば，電荷の符号を測定して区別することができる．しかし2個の電子のように同種の粒子の場合にはこの2つを弁別できない．

粒子の識別不能性によりシステムの状態ベクトルに制約が生じ2種類の影響が現れる．実験的に自然界の粒子はボソン (boson) とフェルミオン (fermion) と呼ぶ2つの異なる性質を持って現れる．ボソンシステムの状態ベクトルはその基本的な識別不能性を反映して，2つの構成要素を置き換えても変化しない．これに対してフェルミオンシステムでは任意の2つの構成要素を入れ替えても状態ベクトルの符号が変化する．両システムとも量子コンピュータで効率良くシミュレートできる．これを行う方法の詳しい説明は本書の範囲を越えているが，その手順はかなり簡単であるとだけ言っておく．間違った対称性の初期状態が与えられた場合は，シミュレーションの開始前に正しい対称性に直すことができる．シミュレーションで使うオペレータは，高次の誤差項の影響も含めて希望する対称性を考慮して構築される．これらの話題を追求してさらなる発展に興味を持つ読者には章末の「歴史と参考資料」欄に指針となる文献が示されている．

**問題 4.1:（計算可能な位相シフト）** $m$ と $n$ は正の整数とする．変換 $f: \{0,\ldots,2^m-1\} \to \{0,\ldots,2^n-1\}$ は $m$ ビットから $n$ ビットに変換する古典的関数であり，3.2.5 項（第I巻）で述べたように $T$ 個の Toffoli ゲートを使って可逆的に計算できる．つまり関数 $(x,y) \to (x, y \oplus f(x))$ は $T$ 個の Toffoli ゲートで実現できる．$2T+n$ 個（またはそれ以下）の 1-，2-，3 - q ビットゲートを用いて，次式で定義されるユニタリー演算を実行する量子回路を与えよ．

$$|x\rangle \to \exp\left(\frac{-2i\pi f(x)}{2^n}\right)|x\rangle. \tag{4.116}$$

**問題 4.2:** $C^n(X)$ ゲートに対する深さ $O(\log n)$ の構成を見出せ．（コメント：回路の深さ (depth) とはゲートを適用する異なる時間ステップの数である．この問題の要点は同じ時間ステップ内に多数のゲートを並行して適用することにより，$C^n(X)$ の構成を並列化できる点にある.）

**問題 4.3:（別の普遍性構築）** $U$ は $n$ 個の q ビットに働くユニタリー行列であるとする．$H \equiv i\ln(U)$ を定義する．次の事項を示せ．

(1) $H$ は 0 から $2\pi$ の範囲に固有値を持つ Hermite オペレータである．

(2) $H$ は次のように書ける：

$$H = \sum_g h_g g, \tag{4.117}$$

ここで $h_g$ は実数，総和は Pauli の行列 $\{I, X, Y, Z\}$ のすべての $n$ 重テンソル積 $g$ について行う．

(3) ある正の整数 $k$ に対して $\Delta = 1/k$ とする．$O(n)$ 個の 1 - および 2 - q ビット演算を用いて，ユニタリー演算 $\exp(-ih_g g\Delta)$ を実行する方法を説明せよ．

(4) 次式を示せ．

$$\exp(-iH\Delta) = \prod_g \exp(-ih_g g\Delta) + O(4^n \Delta^2), \tag{4.118}$$

ここで積は任意の固定した順序による Pauli の行列の $n$ 重テンソル積 $g$ について行う．

(5) 次式を示せ．

$$U = \left[\prod_g \exp(-ih_g g\Delta)\right]^k + O(4^n \Delta). \tag{4.119}$$

(6) $O(n16^n/\epsilon)$ 個の 1 - および 2 - q ビットユニタリー演算を用いて距離 $\epsilon > 0$ 以内で $U$ を近似する方法を説明せよ．

**問題 4.4:**（**最小限の Toffoli ゲート構築**）（**研究**）

(1) Toffoli ゲートを実行するのに要する 2 - q ビットゲートの最小数は何か？

(2) Toffoli ゲートを実行するのに要する 1 - q ビットゲートと制御 NOT ゲートの最小数は何か？

(3) Toffoli ゲートを実行するのに要する 1 - q ビットゲートと制御 $Z$ ゲートの最小数は何か？

**問題 4.5:**（**研究**） シミュレートするのに $n$ の超多項式数の演算を必要とする $n$ - q ビットに働く Hamiltonian 族 $\{H_n\}$ を構築せよ．（コメント：この問題は極めて難しい．）

**問題 4.6:（もつれに基づく普遍性）** 制御 NOT ゲートと単一 q ビットゲートは量子論理ゲートの普遍的集合である．単一 q ビットユニタリーゲートと，Bell 基底で q ビット対を測定する能力と，任意の 4 個の q ビットもつれ状態を作る能力により別の普遍的ゲート集合が構成できることを示せ．

**第 4 章のまとめ: 量子回路**

**普遍性** ：$n$ 個の q ビットへのユニタリー演算は，単一 q ビットゲートと制御 NOT ゲートで正確に実行できる．

**離散的集合による普遍性** ：Hadamard ゲート，位相ゲート，制御 NOT ゲートおよび $\pi/8$ ゲートは，これらのゲートだけで構成される回路を使って $n$ 個の q ビットに働く任意のユニタリー変換が任意の精度 $\epsilon > 0$ で近似できるという意味で，量子計算の**普遍的**ゲートである．このリストの中で $\pi/8$ ゲートを Toffoli ゲートで置き換えたものも普遍的ゲート族となる．

**すべてのユニタリー変換が効率良く実行できるわけではない** ：$n$ 個の q ビットに働くユニタリー演算において任意の有限ゲート集合を用いて距離 $\epsilon$ 以内で近似するのに，$\Omega(2^n \log(1/\epsilon)/\log(n))$ 個のゲート必要とするものも存在する．

**シミュレーション** ：効率的量子回路が構築できる $H_k$ を多項式数加え合わせた総和で表せる Hamiltonian $H = \sum_k H_k$ に対して，$|\psi(0)\rangle$ が与えられると量子コンピュータが時間発展 $e^{-iHt}$ を効率良くシミュレートできて，$|\psi(t)\rangle = e^{-iHt}|\psi(0)\rangle$ が近似できる．

## 歴史と参考資料

本章のゲート構築には広範囲の文献を参考にした．Barenco, Bennett, Cleve, DiVincenzo, Margolus, Shor, Sleator, Smolin, Weinfurter [BBC+95] の論文は本章の多くの回路構成と，単一 q ビットと制御 NOT ゲートに対する普遍性証明に

関する情報源である．もう 1 つの見識のある量子回路の有益な情報源は Beckman, Chari, Devabhaktuni, Preskill の論文 [BCDP96] である．やさしく読み易い入門が DiVincenzo [DiV98] によって書かれている．測定と制御 q ビット端子が可換であるという事実は Griffiths と Niu によって指摘された [GN96].

2 準位ユニタリー変換に対する普遍性証明は Reck, Zeilinger, Bernsein, Bertani [RZBB94] による．制御 NOT と単一 q ビットゲートの普遍性は DiVincenzo により証明された [DiV95b]．演習 4.44 の普遍的ゲート $G$ は Deutsch のゲートと呼ぶことがある [Deu89]．Deutsch, Barenco, Ekert [DBE95] と Lloyd [Llo95] は独立にほとんど如何なる 2 - q ビット量子論理ゲートも普遍的であることを証明した．一連のゲートで生じた誤差がたかだか各ゲートの誤差の和で与えられるということは，Bernstein, Vazirani により証明された [BV97]．我々が注目した普遍的ゲート集合— Hadamard，位相，制御 NOT，$\pi/8$ ゲート — が普遍的であることは Boykin, Mor, Pulver, Roychowdhury, Vatan [BMP+99] が証明し，その論文には $\cos(\theta/2) \equiv \cos^2(\pi/8)$ で定義される $\theta$ が $\pi$ の無理数倍であることの証明も示されている．4.5.4 項の有界性の議論は Knill の論文 [Kni95] によっており，そこには任意のユニタリー演算を量子回路で近似する際の困難性について詳しく調べられている．特に Knill は我々よりも厳密で一般的な限界を得ており，我々が考えた有限集合だけでなく，彼の解析は連続ゲートの普遍的集合の場合にも適用できる．

計算の量子回路モデルは Deutsch[Deu89] によるものであり，その後 Yao が発展させた [Yao93]．後者の論文は計算の量子回路モデルが量子 Turing 機械モデルと等価であることを示した．量子 Turing 機械は 1980 年に Benioff [Ben80] が導入し，Deutsch [Deu85] と Yao [Yao93] が発展させ，現代的な定義は Bernstein と Vazirani [BV97] により与えられた．最後の 2 つの論文は古典計算量理論と類似な量子計算量理論の立ち上げに向けた第 1 歩ともなっている．特に内包関係 **BQP** $\subseteq$ **PSPACE** ともう少し強い結果は Bernstein と Vazirani によって証明された．Knill と Laflamme [KL99] は量子計算量と古典計算量の興味ある関係を発展させた．量子計算量に関するその他の興味ある論文には Adleman, Demarrais, Huang [ADH97] および Watrous [Wat99] の論文がある．後者は「相互作用証明システム」を設定するのに量子コンピュータが古典コンピュータよりも強力であることを示唆する興味深い証拠が記されている．

非計算基底を初期状態とすると量子回路モデルを越える計算能力が得られることは，Daniel Gottesman と Michael Nielsen が示唆した [私信].

量子コンピュータが古典コンピュータよりも効率良く量子システムをシミュレーションできることは 1980 年に Manin [Man80] によって暗示され，それと独立に 1982 年に Feynman [Fey82] により詳しく発展させられた．その後もっと詳しい研究が Abrams と Lloyd [AL97]，Boghosian と Taylor [BT97]，Sornborger と Stewart [SS99]，Wiesner [Wie96] および Zalka [Zal98] によって行われた．Trotter の公式は Trotter [Tro59] によるものであり，Chernoff [Che68] によっても証明された．もっともユニタリーオペレータに対する簡単な形はもっと古く Sophus Lie の時代に遡る．Baker-Campbell-Hausdorff の公式の 3 次形式 (4.104) は Sornborger と Stewart [SS99] により与えられた．Abrams と Lloyd [AL97] は量子コンピュータ上の多体フェルミシステムのシミュレーション手続きを与えた．Terhal と DiVincenzo [TD98] は量子システムが Gibbs 状態に平衡化するシミュレーションの問題を扱った．コラム 4.2 に示した Schrödinger 方程式シミュレーションの方法は Zalka [Zal98] と Wiesner [Wie96] による．

演習 4.25 は Vandersypen によるものでり，Chau と Wilczek による論文 [CW95] にも関連している．演習 4.45 は Boykin, Mor, Pulver, Roychowdhury, Vatan [BMP+99] による．問題 4.2 は Gottesman による．問題 4.6 は Gottesman と Chuang [GC99] による．

# 第5章　量子Fourier変換とその応用

もしも量子コンピュータができたなら
何処にいるスパイも欲しがるだろう
どんな暗号も破れたなら
彼らは e メールも読んでしまう
量子暗号を作って彼らをくじくまで
— Jennifer Sor, Peter Shor

我々の e メールを覗くとは，なんと卑劣な
スパイと量子機械であることか，
でも，がっかりしなくてもよい
彼らはまだ知らない
12 桁や 15 桁の素因数分解の仕方を
— Volker Strassen

詩や音楽の創作と同様に，コンピュータプログラムも芸術だ．
— Donald Knuth

今日までの量子計算における最も目覚ましい発見は，古典コンピュータにできない幾つかのタスクを量子コンピュータが効率良く実行できたことである．例えば $n$ ビット整数の素因数分解は，本書執筆時点で最良の古典アルゴリズム— いわゆる**数体ふるい法** (number field sieve) — によって $\exp(\Theta(n^{1/3}\log^{2/3} n))$ 回の演算を必要とすると考えられている．このサイズは素因数分解する数の指数関数であり，あまり大きくない数に対しても急速に演算が不可能になるので，一般に

素因数分解は古典コンピュータ上で取り扱えない問題と考えられている．これに対して量子アルゴリズムでは，同じタスクを $O(n^2 \log n \log\log n)$ 回の演算で達成できる．つまり知られている最良の古典アルゴリズムに比べて量子コンピュータは**指数関数的**に速く数の素因数分解ができる．この結果それ自身が重要であるだけでなく，多分最も重要な側面はそれが提起する次の疑問である： 古典コンピュータで解けない他のどのような問題が，量子コンピュータで効率良く解けるのだろうか？

本章では量子素因数分解やその他多くの興味ある量子アルゴリズムの鍵となる構成要素である，**量子 Fourier 変換** (quantum Fourier transform) を詳しく説明する．この量子 Fourier 変換は，量子力学的振幅に対して Fourier 変換を実行するための効率的な量子アルゴリズムであり，5.1 節から始める．これにより古典的データの Fourier 変換を計算する古典的タスクが高速化されることにはならない．しかし量子 Fourier 変換が可能にする重要なタスクには，5.2 節で述べるようにある状況下でユニタリーオペレータの固有値を近似する，**位相推定** (phase estimation) がある．これによりさらに他の幾つかの興味ある問題 — **位数発見問題** (order-finding problem) や**素因数分解** (factoring problem) 等 — が解けるようになる．これについて 5.3 節で説明する．位相推定と量子探索アルゴリズムを組み合わせると，次章で述べる探索問題の**解を数える** (counting solutions) 問題を解くことができる．章の最後として 5.4 節では量子 Fourier 変換を用いて**隠れ部分群問題** (hidden subgroup problem) を解くことを議論する．この問題は位相推定や位数発見問題を一般化したものであり，その特別な場合として古典コンピュータ上で取り扱えないと考えられるもう 1 つの問題である，**離散対数問題** (discrete logarithm problem) を効率的に解く量子アルゴリズムが含まれている．

## 5.1　量子 Fourier 変換

> 良いアイディアとはそれ自身がより単純になると同時に，最初目指した以外の問題も解けるようになるものだ． — Robert Tarjan

数学やコンピュータ科学の問題を解く際の最も便利な方法は，すでに解がわかっている何か他の問題にそれを**変換**することである．多くの異なる状況でこのタイ

プの変換にしばしば出現するので，それ自身が研究対象となっているものが幾つかある．量子計算における偉大な発見は，このような変換の幾つかが古典コンピュータよりも早く量子コンピュータで計算できることであり，この発見により量子コンピュータ向けの高速アルゴリズムが構築可能になった．

そのような変換の 1 つが**離散 Fourier 変換** (discrete Fourier transform) である．通常の数学表記では離散 Fourier 変換は複素数 $x_0, \ldots, x_{N-1}$ のベクトルを入力として取り込む．ここでベクトルの長さ $N$ は定まったパラメータである．その出力は

$$y_k \equiv \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi ijk/N} \tag{5.1}$$

で定義される，複素数 $y_0, \ldots, y_{N-1}$ のベクトルで表される変換データである．

**量子 Fourier 変換** (quantum Fourier transform) は全く同じ変換であるが，その慣用的表現は少し違っている．正規直交基底 $|0\rangle, \ldots, |N-1\rangle$ 上の量子 Fourier 変換は基底状態に次の作用をする線形オペレータとして定義される．

$$|j\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi ijk/N} |k\rangle. \tag{5.2}$$

同じことであるが，任意の状態に対する作用は次のように書ける．

$$\sum_{j=0}^{N-1} x_j |j\rangle \rightarrow \sum_{k=0}^{N-1} y_k |k\rangle, \tag{5.3}$$

ここで振幅 $y_k$ は振幅 $x_j$ の離散 Fourier 変換である．この定義から明らかではないが，この変換はユニタリー変換であり，したがって量子コンピュータにおけるダイナミクスとして実現できる．我々は Fourier 変換を計算する明らかにユニタリーな量子回路を構築することによって，Fourier 変換のユニタリー性を実証しよう．Fourier 変換がユニタリーであることを直接証明することも容易である：

**演習 5.1:** 式 (5.2) で定義される線形変換がユニタリーであることを直接証明せよ．

**演習 5.2:** $n$ 個の q ビット状態 $|00\ldots0\rangle$ の Fourier 変換を陽に計算せよ．

これ以後 $N = 2^n$，$n$ はある整数とし，基底 $|0\rangle, \ldots, |2^n - 1\rangle$ は $n$ 個の q ビットの量子コンピュータに対する計算基底とする．状態 $|j\rangle$ を 2 進数表現 (binary representation) で $j = j_1 j_2 \ldots j_n$ と書くと便利である．形式的には $j = j_1 2^{n-1} + j_2 2^{n-2} + \cdots + j_n 2^0$ である．また **2 進小数** (binary fraction) $j_l/2 + j_{l+1}/4 + \cdots + j_m/2^{m-l+1}$ を表す記号 $0.j_l j_{l+1} \ldots j_m$ を採用すると便利である．

簡単な代数計算で，量子 Fourier 変換の便利な**積表現** (product representation) が次のように与えられる：

$$|j_1, \ldots, j_n\rangle \to \frac{\left(|0\rangle + e^{2\pi i 0.j_n}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0.j_{n-1}j_n}|1\rangle\right)\cdots\left(|0\rangle + e^{2\pi i 0.j_1 j_2 \cdots j_n}|1\rangle\right)}{2^{n/2}}. \tag{5.4}$$

この積表現は便利なので，これを量子 Fourier 変換の**定義**と考えたくなるほどである．この表現により，Fourier 変換を計算する効率的量子回路を構築して，量子 Fourier 変換がユニタリーであることが証明できる．さらに量子 Fourier 変換に基づくアルゴリズムの見通しも得ることができる．また偶然のおまけとして古典的高速 Fourier 変換も得られることを演習で示す．

積表現 (5.4) と定義 (5.2) が等価であることは次の簡単な代数計算で導ける：

$$|j\rangle \to \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} 2^{2\pi i jk/2^n}|k\rangle \tag{5.5}$$

$$= \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} \cdots \sum_{k_n=0}^{1} e^{2\pi i j(\sum_{l=1}^{n} k_l 2^{-l}}|k_1 \ldots k_n\rangle \tag{5.6}$$

$$= \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} \cdots \sum_{k_n=0}^{1} \bigotimes_{l=1}^{n} e^{2\pi i j k_l 2^{-l}}|k_l\rangle \tag{5.7}$$

$$= \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} \left[\sum_{k_l=0}^{1} e^{2\pi i j k_l 2^{-l}}|k_l\rangle\right] \tag{5.8}$$

$$= \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} \left[|0\rangle + e^{2\pi i j 2^{-l}}|1\rangle\right] \tag{5.9}$$

$$= \frac{\left(|0\rangle + e^{2\pi i 0.j_n}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0.j_{n-1}j_n}|1\rangle\right)\cdots\left(|0\rangle + e^{2\pi i 0.j_1 j_2 \cdots j_n}|1\rangle\right)}{2^{n/2}}. \tag{5.10}$$

積表現 (5.4) によって量子 Fourier 変換に対する効率的回路が容易に導ける．この回路を図 5.1 に示す．ゲート $R_k$ は次のユニタリー変換を表す．

$$R_k \equiv \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{bmatrix}. \tag{5.11}$$

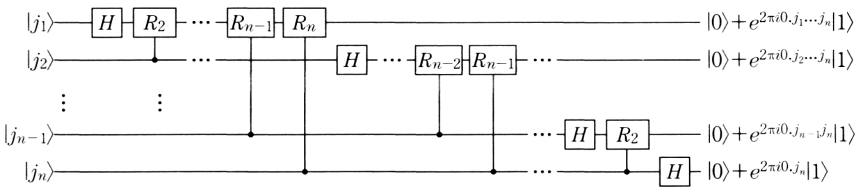


図 5.1: 量子 Fourier 変換の効率的回路．この回路は量子 Fourier 変換に対する積表現式 (5.4) から容易に導ける．回路の最後の交換ゲートは図に示されていないが，q ビットの順序を反転する．出力の正規化係数 $1/\sqrt{2}$ も示されていない．

図の回路が量子 Fourier 変換を実行することを確かめるために，$|j_1 \dots j_n\rangle$ を入力したときに何が起きるかを考える．最初のビットに Hadamard ゲートを適用すると $j_1 = 1$ ならば $e^{2\pi i 0.j_1} = -1$，そうでなければ $+1$ なので次の状態が作られる：

$$\frac{1}{2^{1/2}}\left(|0\rangle + e^{2\pi i 0.j_1}|1\rangle\right)|j_2 \dots j_n\rangle. \tag{5.12}$$

制御 $R_2$ ゲートを適用すると次の状態が作られる：

$$\frac{1}{2^{1/2}}\left(|0\rangle + e^{2\pi i 0.j_1 j_2}|1\rangle\right)|j_2 \dots j_n\rangle. \tag{5.13}$$

制御 $R_3$，$R_4, \dots, R_n$ ゲートを順次適用すると，そのたびに最初の $|1\rangle$ の係数の位相に追加ビットが加わる．この手続きが終わると状態は次のようになる：

$$\frac{1}{2^{1/2}}\left(|0\rangle + e^{2\pi i 0.j_1 j_2 \dots j_n}|1\rangle\right)|j_2 \dots j_n\rangle. \tag{5.14}$$

次に第 2 - q ビットに同様の手続きを実行する．Hadamard ゲートによって状態は次のように変化する：

$$\frac{1}{2^{2/2}}\left(|0\rangle + e^{2\pi i 0.j_1 j_2 \dots j_n}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0.j_2}|1\rangle\right)|j_3 \dots j_n\rangle. \tag{5.15}$$

制御 $R_2, \ldots, R_{n-1}$ ゲートを適用すると得られる状態は：

$$\frac{1}{2^{2/2}}\Big(|0\rangle + e^{2\pi i 0.j_1 j_2 \ldots j_n}|1\rangle\Big)\Big(|0\rangle + e^{2\pi i 0.j_2 \ldots j_n}|1\rangle\Big)|j_3 \ldots j_n\rangle. \tag{5.16}$$

この操作を各 q ビットに対して行うと最終状態は：

$$\frac{1}{2^{n/2}}\left(|0\rangle + e^{2\pi i 0.j_1 j_2 \ldots j_n}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0.j_2 \ldots j_n}|1\rangle\right)\ldots\left(|0\rangle + e^{2\pi i 0.j_n}|1\rangle\right). \tag{5.17}$$

わかり易くするために図 5.1 から省いたが，次に交換操作（回路の記述については 1.3.4 項（第 I 巻）を参照）を用いて q ビットの順序を反転する．交換操作後の q ビット状態は：

$$\frac{1}{2^{n/2}}\left(|0\rangle + e^{2\pi i 0.j_n}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0.j_{n-1} j_n}|1\rangle\right)\ldots\left(|0\rangle + e^{2\pi i 0.j_1 j_2 \cdots j_n}|1\rangle\right). \tag{5.18}$$

式 (5.4) と比べるとこれが所望の量子 Fourier 変換の出力であることがわかる．回路中の全ゲートはユニタリーなので，これによって量子 Fourier 変換がユニタリーであることも証明される．3 - q ビットに働く量子 Fourier 変換回路の実例をコラム 5.1 に示す．

この回路はゲートを幾つ使うか？ 最初に第 1 の q ビットに対して Hadamard ゲートと $n-1$ 回の条件付き回転を行うので全体で $n$ 個のゲートになる．次に第 2 の q ビットに対して Hadamard ゲートと $n-2$ 個の条件付きゲートを施すので合計 $n+(n-1)$ 個となる．これを続けると $n+(n-1)+\cdots+1 = n(n+1)/2$ 個と交換に必要なゲート数が必要であることがわかる．交換回数はたかだか $n/2$ 回であり，1 回の交換が制御 NOT 回路 3 つで実行できる．したがってこの回路で $\Theta(n^2)$ 回のアルゴリズムにより量子 Fourier 変換ができる．

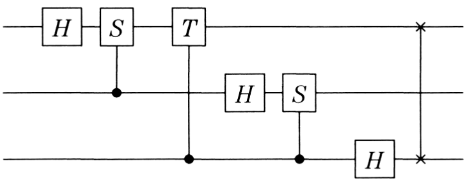
これに対して $2^n$ 個の要素の離散 Fourier 変換を計算する最良の古典アルゴリズムは**高速 Fourier 変換** (FFT; fast Fourier transform) であり，$\Theta(n2^n)$ 個のゲートで離散 Fourier 変換を計算することができる．つまり古典コンピュータで Fourier 変換を計算するには，量子コンピュータ上での量子 Fourier 変換に比べて指数関数的に多くの演算が必要になる．

Fourier 変換は多くの実世界のデータ処理応用に重要なステップなので，一見この高速化は素晴らしいものに見える．例えば，コンピュータによる音声認識では

音素認識の最初のステップはディジタル化された音声を Fourier 変換する．この Fourier 変換の計算を高速化するために量子 Fourier 変換が利用できるであろうか？ 残念ながらその方法は知られていないというのが答である．問題は量子コンピュータにおいて振幅を直接測定して利用できない点にある．したがって，元の状態の Fourier 変換された振幅を決定する方法がない．さらに悪いことに Fourier 変換すべき元の状態を効率良く作り出す方法が一般的には知られていない．したがって，我々の期待に反して量子 Fourier 変換の用途を見つけるのはかなり微妙なところである．本章と次章で量子 Fourier 変換を巧妙に応用した幾つかのアルゴリズムを詳しく説明する．

**コラム 5.1: 3 - q ビットの量子 Fourier 変換**

3 個の q ビットの量子 Fourier 変換に対応する回路を明示的に示すことは問題の具体化に役立つ：




$S$ と $T$ は位相ゲートと $\pi/8$ ゲートである．この場合の量子 Fourier 変換を行列として陽に書き表すと，$\omega = e^{2\pi i/8} = \sqrt{i}$ として

$$\frac{1}{\sqrt{8}}\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & \omega^7 \\ 1 & \omega^2 & \omega^4 & \omega^6 & 1 & \omega^2 & \omega^4 & \omega^6 \\ 1 & \omega^3 & \omega^6 & \omega & \omega^4 & \omega^7 & \omega^2 & \omega^5 \\ 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 \\ 1 & \omega^5 & \omega^2 & \omega^7 & \omega^4 & \omega & \omega^6 & \omega^3 \\ 1 & \omega^6 & \omega^4 & \omega^2 & 1 & \omega^6 & \omega^4 & \omega^2 \\ 1 & \omega^7 & \omega^6 & \omega^5 & \omega^4 & \omega^3 & \omega^2 & \omega \end{bmatrix}. \tag{5.19}$$

**演習 5.3:（古典的高速 Fourier 変換）** 古典コンピュータを用いて $2^n$ 個の複素数を含むベクトルの Fourier 変換を行う．式 (5.1) の直接評価に基づいて Fourier 変換を実直に行う方法では，$\Theta(2^{2n})$ 回の基本的算術演算を必要とすることを証明せよ．式 (5.4) を使って $\Theta(n2^n)$ 回に減らす方法を見出せ．

**演習 5.4:** 制御 $R_k$ ゲートを単一 q ビットゲートと制御 NOT ゲートに分解せよ．

**演習 5.5:** 量子 Fourier 逆変換を行う量子回路を与えよ．

**演習 5.6:（近似的量子 Fourier 変換）** 量子 Fourier 変換の量子回路を構築する際に，ゲートには使用 q ビット数に応じて指数関数的な精度が見かけ上要求される．しかしそのような精度は多項式サイズの量子回路に要求されたことはない．例えば，$U$ は $n$ - q ビットの理想的量子 Fourier 変換であり，$V$ は制御 $R_k$ ゲートが $\Delta = 1/p(n)$ の精度（$p(n)$ はある多項式）で実行されたときの変換である．このとき誤差 $E(U,V) \equiv \max_{|\psi\rangle} \|(U-V)|\psi\rangle\|$ は $\Theta(n^2/p(n))$ で変化し，したがって各ゲートが多項式精度で動作するならば出力状態の多項式精度が保証されることを示せ．

## 5.2　位相推定

Fourier 変換は**位相推定** (phase estimation) と呼ぶ一般的手続きの鍵であり，その位相推定は多くの量子アルゴリズムの鍵である．ユニタリーオペレータ $U$ が固有値 $e^{2\pi i\varphi}$ と固有ベクトル $|u\rangle$ を有するとする．ここで $\varphi$ の値は未知である．位相推定アルゴリズムのゴールは $\varphi$ を推定することである．推定をするために適切な負でない整数 $j$ に対して状態 $|u\rangle$ を準備し，制御 $U^{2^j}$ 演算を行う**ブラックボックス**（**オラクル** (oracle) とも呼ぶ）が使えるとする．ブラックボックスを使うということは，位相推定の手続きが本来完全な量子アルゴリズムでないということである．むしろ位相推定は「サブルーチン」または「モジュール」と考え，他のサブルーチンと組み合わせて興味ある計算タスクができると考えるほうがよい．位相推定手続きの特定の応用で我々はこれを正確に行う．すなわち，ブラックボックス演算を如何に行うかを記述し，これを位相推定手続きと組み合わせて真に有用なタスクを行うのである．しかし当面はこれらをブラックボックスであると想像することにする．

量子位相推定の手続きには2つのレジスタを使う．第1レジスタは最初に状態 $|0\rangle$ にある $t$ 個の q ビットを収容する．$t$ を選ぶ際に考慮すべきことは2つある：$\varphi$ を推定する際に望む精度のディジット数と位相推定手続きが成功する確率である．$t$ がこれらの量にどう依存するかは次に続く解析から自然にわかる．

第2レジスタは状態 $|u\rangle$ から出発し，これは $|u\rangle$ を蓄積するに必要な数の q ビットを含んでいる．位相推定は2段階で実行する．最初に図5.2に示す回路を適用する．この回路は第1レジスタに Hadamard 変換を適用し，続いて第2レジスタに制御 $U$ 演算を適用し，$U$ のベキを順次2ずつ引き上げる．第1レジスタの最終状態は次式で与えられることが容易にわかる．

$$\frac{1}{2^{t/2}}\left(|0\rangle + e^{2\pi i 2^{t-1}\varphi}|1\rangle\right)\left(|0\rangle + e^{2\pi i 2^{t-2}\varphi}|1\rangle\right)\cdots\left(|0\rangle + e^{2\pi i 2^{0}\varphi}|1\rangle\right)$$
$$= \frac{1}{2^{t/2}}\sum_{k=0}^{2^t-1} e^{2\pi i\varphi k}|k\rangle. \quad (5.20)$$

第2レジスタは計算の間を通じて $|u\rangle$ なので，この記述では第2レジスタは省略した．

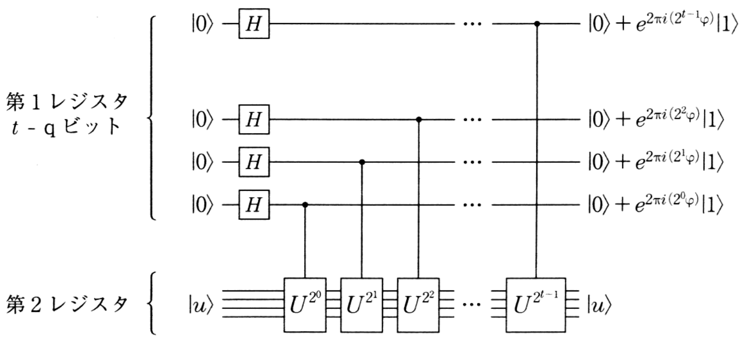



**図 5.2:** 位相推定手続きの第1段階．右側の式で正規化係数 $1/\sqrt{2}$ を省略した．

**演習 5.7:** 図5.2の一連の制御 $U$ 演算の効果は，状態 $|j\rangle|u\rangle$ を $|j\rangle U^j|u\rangle$ に変換するものであることを示せ．これによって図5.2の回路への見通しがよくなる．（これは $|u\rangle$ が $U$ の固有状態であることに依存しない．）

位相推定の第2段階は第1レジスタに量子 Fourier 逆変換 (inverse quantum Fourier transform) を行うことである．これは前節で示したように（演習5.5），

量子 Fourier 変換の回路を逆にして $\Theta(t^2)$ ステップで実現できる．最後に位相推定の 3 番目の段階では，計算基底で測定を行い第 1 レジスタの状態を読み取る．これによりかなり良く $\varphi$ を推定できることを示そう．アルゴリズムの全体図を図 5.3 に示す．

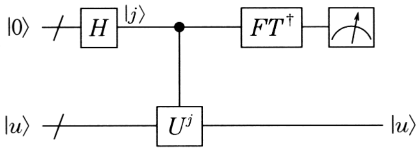



**図 5.3:** 位相推定手続き全体の模式図．上の q ビット（「/」はいつものように配線の束を表す）は第 1 レジスタ，下の q ビットは第 2 レジスタを示し，その数は $U$ を実行するのに必要な数とする．$|u\rangle$ は $U$ の固有状態，固有値は $e^{2\pi i\varphi}$ である．測定出力は $\varphi$ の近似であり，精度は $t - \lceil\log(2+\frac{1}{2\epsilon})\rceil$ ビット，成功の確率は少なくとも $1-\epsilon$ である．

位相推定がなぜうまくいくのかを直観的に理解するために，$\varphi$ が $\varphi = 0.\varphi_1 \dots \varphi_t$ というように正確に $t$ ビットで与えられるとする．このとき位相推定の第 1 段階から生じる状態 (5.20) を書き換えると

$$\frac{1}{2^{t/2}}\left(|0\rangle + e^{2\pi i 0.\varphi_t}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0.\varphi_{t-1}\varphi_t}|1\rangle\right)\cdots\left(|0\rangle + e^{2\pi i 0.\varphi_1\varphi_2\cdots\varphi_t}|1\rangle\right). \tag{5.21}$$

位相推定の第 2 段階では量子 Fourier 逆変換を施す．いまの結果と Fourier 変換の積表現 (5.4) を比較すると，第 2 段階の出力状態は積状態 $|\varphi_1 \dots \varphi_t\rangle$ であることがわかる．したがって計算基底で測定すると正確に $\varphi$ が得られる！

まとめると，位相推定アルゴリズムによって，対応する固有ベクトル $|u\rangle$ で与えられるユニタリーオペレータ $U$ の固有値の位相 $\varphi$ を推定できる．この手続きの核心を成す重要な点は次の変換を実行する Fourier 逆変換にある．

$$\frac{1}{2^{t/2}}\sum_{j=0}^{2^t-1} e^{2\pi i\varphi j}|j\rangle|u\rangle \to |\tilde{\varphi}\rangle|u\rangle, \tag{5.22}$$

ここで $|\tilde{\varphi}\rangle$ は測定されたとき $\varphi$ の良い推定量を与える状態を表す．

### 5.2.1 性能と要求条件

上述の解析は $\varphi$ が正確に $t$ ビットの 2 進数展開で書ける理想的な場合に適用される．理想的でない場合に何がおきるか？ 式 (5.22) の表記から予見できるように，我々が述べた手続きは高い確率で $\varphi$ のかなり良い近似を与えることを明らかにしよう．これを示すには注意深い取り扱いが必要になる．

$b$ を 0 から $2^t - 1$ の範囲の整数として，$b/2^t = 0.b_1 \dots b_t$ が $\varphi$ より小さく $\varphi$ の最良の $t$ ビット近似になるように選ぶとする．つまり $\varphi$ と $b/2^t$ の差 $\delta \equiv \varphi - b/2^t$ は $0 \leq \delta \leq 2^{-t}$ を満たす．我々の目的は位相推定手続きの最後の観測が $b$ に近い結果を与え，高い確率で $\varphi$ を正確に推定できることを示すことにある．量子 Fourier 逆変換を状態 (5.20) に適用すると，次の状態が得られる：

$$\frac{1}{2^t}\sum_{k,l=0}^{2^t-1} e^{\frac{-2\pi i k l}{2^t}} e^{2\pi i \varphi k}|l\rangle. \tag{5.23}$$

$\alpha_l$ を $|(b+l)(\mathrm{mod}\ 2^t)\rangle$ の振幅とすると

$$\alpha_l \equiv \frac{1}{2^t}\sum_{k=0}^{2^t-1}\left(e^{2\pi i(\varphi-(b+l)/2^t)}\right)^k. \tag{5.24}$$

これは幾何級数なので

$$\alpha_l = \frac{1}{2^t}\left(\frac{1-e^{2\pi i(2^t\varphi-(b+l))}}{1-e^{2\pi i(\varphi-(b+l)/2^t)}}\right) \tag{5.25}$$

$$= \frac{1}{2^t}\left(\frac{1-e^{2\pi i(2^t\delta-l)}}{1-e^{2\pi i(\delta-l/2^t)}}\right). \tag{5.26}$$

最終測定結果を $m$ とする．我々の目的は $|m-b| > e$ となる値 $m$ を得る確率の限界を与えることである．ここで $e$ は所望の許容誤差を特徴付ける正の整数である．そのような $m$ を観測する確率は次式で与えられる：

$$p(|m-b|>e) = \sum_{-2^{t-1}<l\leq-(e+1)}|\alpha_l|^2 + \sum_{e+1\leq l\leq 2^{t-1}}|\alpha_l|^2. \tag{5.27}$$

しかし任意の実数 $\theta$ に対して $|1-\exp(i\theta)| \leq 2$ なので

$$|\alpha_l| \leq \frac{2}{2^t|1-e^{2\pi i(\delta-l/2^t)}|}. \tag{5.28}$$

初歩的な幾何学あるいは解析学より，$-\pi \le \theta \le \pi$ ならば常に $|1-\exp(i\theta)| \ge 2|\theta|/\pi$ である．しかし $-2^{t-1} < l \le 2^{t-1}$ のときに $-\pi \le 2\pi(\delta - l/2^t) \le \pi$ となる．したがって

$$|\alpha_l| \le \frac{1}{2^{t+1}(\delta - l/2^t)}. \tag{5.29}$$

式 (5.27) と式 (5.29) を組み合わせると

$$p(|m-b|>e) \le \frac{1}{4}\left[\sum_{l=-2^{t-1}+1}^{-(e+1)} \frac{1}{(l-2^t\delta)^2} + \sum_{l=e+1}^{2^{t-1}} \frac{1}{(l-2^t\delta)^2}\right]. \tag{5.30}$$

$0 \le 2^t\delta \le 1$ を思い出すと

$$p(|m-b|>e) \le \frac{1}{4}\left[\sum_{l=-2^{t-1}+1}^{-(e+1)} \frac{1}{l^2} + \sum_{l=e+1}^{2^{t-1}} \frac{1}{(l-1)^2}\right] \tag{5.31}$$

$$\le \frac{1}{2}\sum_{l=e}^{2^{t-1}-1} \frac{1}{l^2} \tag{5.32}$$

$$\le \frac{1}{2}\int_{e-1}^{2^{t-1}-1} dl \frac{1}{l^2} \tag{5.33}$$

$$= \frac{1}{2(e-1)}. \tag{5.34}$$

精度 $2^{-n}$ で $\varphi$ を近似する，つまり $e = 2^{t-n} - 1$ と選ぶ．位相推定アルゴリズムで $t = n + p$ 個の q ビットを使用すると，式 (5.34) からこの精度で正しい近似を得る確率は少なくとも $1 - 1/2(2^p - 2)$ であることがわかる．したがって，$n$ ビット精度で少なくとも $1 - \epsilon$ の成功確率で正確に $\varphi$ を得るには

$$t = n + \left\lceil \log\left(2 + \frac{1}{2\epsilon}\right) \right\rceil. \tag{5.35}$$

位相推定アルゴリズムを利用するには，$U$ の固有状態 $|u\rangle$ を用意できなければならない．そのような固有状態の準備の仕方がわからなければどうなるか？ $|u\rangle$ の代わりに何か他の状態 $|\psi\rangle$ を準備したとする．この状態を $U$ の固有状態 $|u\rangle$ で展開すると $|\psi\rangle = \sum_u c_u|u\rangle$ を得る．固有状態 $|u\rangle$ は固有値 $e^{2\pi i\varphi_u}$ を持つとする．直観的に言って位相推定アルゴリズムを走らせると，その結果は $\sum_u c_u|\widetilde{\varphi_u}\rangle|u\rangle$ に

近い出力が与えられるであろう．ここで $\widetilde{\varphi_u}$ は位相 $\varphi_u$ のかなり良い近似である．したがって，最初のレジスタを読み出すと $\varphi_u$ の良い近似が得られると期待される．ここで $u$ は確率 $|c_u|^2$ でランダムに選ぶ．ここでの議論を厳密化することは演習 5.8 に譲る．この手続きではアルゴリズムに付加的なランダムさを導入するというコストを払って，（多分未知の）固有状態を準備するのが避けられる．

**演習 5.8:** 位相推定アルゴリズムでは状態 $|0\rangle|u\rangle$ を状態 $|\widetilde{\varphi_u}\rangle|u\rangle$ に変換して，与えられた入力 $|0\rangle(\sum_u c_u|u\rangle)$ に対するアルゴリズムの出力が $\sum_u c_u|\widetilde{\varphi_u}\rangle|u\rangle$ となるとしている．もし式 (5.35) に従って $t$ を選ぶと，位相推定アルゴリズムの結論において，$n$ ビット精度で $\varphi$ を測定する確率が少なくとも $|c_u|^2(1-\epsilon)$ となることを示せ．

位相推定はなぜ興味深いのか？ 先ず物理的観点から有意で興味ある問題 — ユニタリーオペレータの固有ベクトルが与えられたとき，それに付随する固有値を推定する方法 — が位相推定自身によって解ける．これが現実に用いられる理由は他の興味ある問題が位相推定に縮約できるところからくる．この点については後の節で示す．位相推定アルゴリズムを以下にまとめておく．

**アルゴリズム：量子位相推定**

**入力：** (1) 整数 $j$ に対して制御 $U^j$ 演算を行うブラックボックス

(2) 固有値 $e^{2\pi i\varphi_u}$ を持つ $U$ の固有状態 $|u\rangle$

(3) $|0\rangle$ に初期化された $t = n + \lceil\log(2+\frac{1}{2\epsilon}\rceil$ 個の q ビット

**出力：** $\varphi_u$ に対する $n$ ビット近似 $\widetilde{\varphi_u}$

**演算回数：** $O(t^2)$ 回の演算と 1 回の制御 $U^j$ ブラックボックス呼び出し．成功確率は少なくとも $1-\epsilon$

**手続き：**

**1**. $|0\rangle|u\rangle$ 初期状態

**2**. $\rightarrow \frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}|j\rangle|u\rangle$ 重ね合せ

**3.** $\rightarrow \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} |j\rangle U^j |u\rangle$ 　ブラックボックスを適用

$= \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} e^{2\pi i j \varphi_u} |j\rangle |u\rangle$ 　ブラックボックスの結果

**4.** $\rightarrow |\widetilde{\varphi_u}\rangle |u\rangle$ 　Fourier 逆変換を適用

**5.** $\rightarrow \widetilde{\varphi_u}$ 　第 1 レジスタを測定

**演習 5.9:** $U$ は固有値 $\pm 1$ を有するユニタリー変換であり，状態 $|\psi\rangle$ に作用するとする．位相推定手続きを使って，$|\psi\rangle$ を $U$ の 2 つの固有空間の一方または他方に収縮させる量子回路を構築し，最終状態がどの空間にあるかを示す古典的表現を与えよ．その結果を演習 4.43 と比較せよ．

## 5.3　応用：位数発見と素因数分解

位相推定の手続きを使っていろいろな興味深い問題を解くことができる．ここではこれらの問題の中で最も興味ある 2 つの問題 — **位数発見問題** (order-finding problem) と**素因数分解問題** (factoring problem) — について述べる．事実これら 2 つの問題は互いに等価であって，5.3.1 項で位数発見問題を解く量子アルゴリズムを説明し，5.3.2 項で位数発見問題が如何にして素因数分解能力をも意味するのかを説明する．

素因数分解や位数発見の量子アルゴリズムを理解するには整数論の素養が求められる．必要な材料はすべて付録 D にまとめてある．次の 2 節は問題の量子的側面に焦点を当てるのでこれを読むのに剰余計算を少し知っていればよい．ここで引用する整数論の結論に対する証明は付録 D に掲載した．

位数発見と素因数分解の高速量子アルゴリズムに興味を持つ理由が少なくとも 3 つある．第 1 は我々が最も重要と考えるもので，量子コンピュータが古典コンピュータよりも本質的に強力と考える証拠を提供し，強い Church-Turing の提唱に対して確かな疑念を提示する．第 2 は量子的であれ古典的であれ両アルゴリズムとも，新たなアルゴリズムへの興味を正当化するに十分な価値を持っている．第 3 は実際的立場から最も重要な点であって，位数発見と素因数分解の効率的ア

ルゴリズムはRSA公開鍵暗号システム（付録E）を破るのに使える．

### 5.3.1 応用：位数発見

$N$ を法とする $x$ の**位数** (order) とは，共通の因数を持たない正の整数 $x$ と $N$（$x < N$）に対して，$x^r = 1 \pmod N$ なる最小の正の整数 $r$ であるとして定義される．位数発見問題はある特定の $x$ と $N$ に対する位数を決定する問題である．位数発見は，問題を規定するのに必要な $O(L)$ ビットに対して多項式のリソースを使って解くアルゴリズムが知られておらず，古典コンピュータ上で困難な問題と信じられている．ここで $L \equiv \lceil \log(N) \rceil$ は $N$ を規定するのに必要なビット数である．本項では位相推定を使って，位数発見の効率的量子アルゴリズムを得る方法を説明する．

**演習 5.10:** $N = 21$ を法とする $x = 5$ の位数は 6 であることを示せ．

**演習 5.11:** $x$ の位数は $r \leq N$ を満たすことを示せ．

位数発見の量子アルゴリズムは，$y \in \{0,1\}^L$ としてユニタリーオペレータ

$$U|y\rangle \equiv |xy \pmod N\rangle \tag{5.36}$$

に適用された位相推定アルゴリズムに他ならない．（これ以降 $N \leq y \leq 2^L - 1$ のとき $xy \pmod N$ は再び $y$ に等しいという慣用に従う．つまり $U$ が有意に作用するのは $0 \leq y \leq N-1$ のときだけである.）簡単な計算により，整数 $0 \leq s \leq r-1$ に対して

$$|u_s\rangle \equiv \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp\left[\frac{-2\pi i s k}{r}\right] |x^k \bmod N\rangle \tag{5.37}$$

により定義された状態は $U$ の固有状態であることがわかる．なぜならば

$$U|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp\left[\frac{-2\pi i s k}{r}\right] |x^{k+1} \bmod N\rangle \tag{5.38}$$

$$= \exp\left[\frac{2\pi i s}{r}\right] |u_s\rangle. \tag{5.39}$$

位相推定手続きを用いると，対応する固有値 $\exp(2\pi i s/r)$ が高い精度で得られ，これから少しの計算で位数 $r$ が得られる．

**演習 5.12:** $U$ がユニタリーであることを示せ．（ヒント：$x$ は $N$ と互いに素 (co-prime) であり，したがって $N$ を法とする逆数 (inverse modulo $N$) を有する．）

位相推定手続きを使うには2つの重要な要件がある：任意の整数 $j$ に対して制御 $U^{2^j}$ 演算を実行する効率の良い手続きがなければならないことと，有意な固有値を持つ固有状態 $|u_s\rangle$，あるいは少なくともそのような固有状態の重ね合せを効率良く準備することである．最初の要件は**剰余指数化** (modular exponentiation) と呼ぶ手続きで満たすことができて，これにより位相推定手続きを進める際の $O(L^3)$ 個のゲートを用いた一連の制御 $U^{2^j}$ 演算がすべて実行できる．これについてはコラム 5.2 で述べる．

**コラム 5.2: 剰余指数化**

位数発見アルゴリズムの一部を成す位相推定手続きに用いる一連の制御 $U^{2^j}$ 演算を如何に計算するか？ それにはまず次の変換を計算してみる：

$$|z\rangle|y\rangle \rightarrow |z\rangle U^{z_t 2^{t-1}} \dots U^{z_1 2^0}|y\rangle \tag{5.40}$$

$$= |z\rangle|x^{z_t 2^{t-1}} \times \cdots \times x^{z_1 2^0} y \pmod N\rangle \tag{5.41}$$

$$= |z\rangle|x^z y \pmod N\rangle. \tag{5.42}$$

このように位相推定に用いる一連の制御 $U^{2^j}$ 演算は，第2レジスタの内容に**剰余指数** (modular exponential) $x^z \pmod N$ を掛けたものと等価である．ここで $z$ は第1レジスタの内容である．この演算は可逆計算のテクニックを用いると容易に実行できる．基本的考えは第3レジスタの $z$ の関数 $x^z \pmod N$ を可逆計算し，第2レジスタの内容に $x^z \pmod N$ を可逆的に乗じ，終了時に逆計算 (uncomputation) のトリックを使って第3レジスタの内容を消去する．

剰余指数の計算アルゴリズムは2段階からなっている．第1段階では剰余の積を使って $N$ を法とする $x$ を2乗して $x^2 \pmod N$ を計算し，$x^2 \pmod N$ を2乗して $x^4 \pmod N$ を計算し，これを続けて $t-1$ までの全 $j$ に対して $x^{2^j} \pmod N$ を計算する．ここで $t = 2L + 1 + \lceil \log(2 + 1/(2\epsilon)) \rceil = O(L)$ を用い，全体で $t - 1 = O(L)$ 回の2乗演算を行う．1回の2乗演算のコスト

が $O(L^2)$ なので（このコストは子供の頃に習った掛け算アルゴリズムを使って 2 乗する回路を仮定している），第 1 段階の全コストは $O(L^3)$ となる．アルゴリズムの第 2 段階はすでに述べた結果に基づいている：

$$\begin{aligned} & x^z (\mathrm{mod}\ N) \\ & \quad = \left(x^{z_t 2^{t-1}} (\mathrm{mod}\ N)\right)\left(x^{z_{t-1} 2^{t-2}} (\mathrm{mod}\ N)\right) \dots \left(x^{z_1 2^0} (\mathrm{mod}\ N)\right). \end{aligned} \tag{5.43}$$

$t-1$ 回の剰余積を各回 $O(L^2)$ のコストで行うと，この積は $O(L^3)$ 個のゲートで計算できることがわかる．これは我々の目的には十分効率的であるが，積に対する効率的アルゴリズムを用いると（「歴史と参考資料」欄参照），より効率的アルゴリズムになる．3.2.5 項（第 I 巻）のテクニックを用いると，$t$ ビットレジスタと $L$ ビットレジスタを有し，初期状態 $(z, y)$ から出発して $O(L^3)$ 個のゲートを用いて $(z, x^z y\ (\mathrm{mod}\ N))$ を出力する可逆回路が簡単に構築できる．またこの回路は $O(L^3)$ 個のゲートを用いて，変換 $|z\rangle|y\rangle \to |z\rangle|x^z y\ (\mathrm{mod}\ N)\rangle$ を計算する量子回路に翻訳することができる．

第 2 の要求条件は少し難しい：$|u_s\rangle$ を準備するには $r$ を知らなければならないがこれは全く不可能である．しかしこの式に注目すれば幸いにも $|u_s\rangle$ を準備する問題を回避できる：

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle = |1\rangle. \tag{5.44}$$

位相推定手続きを進める際に，（図 5.3 を参考にして）もし最初のレジスタに $t = 2L + 1 + \lceil \log(2 + \frac{1}{2\epsilon}) \rceil$ 個の q ビットを用い，第 2 レジスタに状態 $|1\rangle$ — これは容易に作れる — を準備すると，$2L+1$ ビット精度と少なくとも $(1-\epsilon)/r$ の確率で，0 から $r-1$ の範囲の各 $s$ に対して位相推定値 $\varphi \approx s/r$ が得られる．位数発見アルゴリズムを図 5.4 に模式的に示す．

**演習 5.13:** 式 (5.44) を証明せよ．（ヒント：$\sum_{s=0}^{r-1} \exp(-2\pi i s k/r) = r\delta_{k0}$ ．）

実際には次式を証明せよ．

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{2\pi i s k/r} |u_s\rangle = |x^k \bmod N\rangle. \tag{5.45}$$

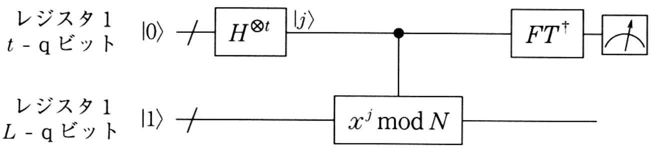



**図 5.4:** 位数発見アルゴリズムの量子回路．第 2 レジスタは状態 $|1\rangle$ に初期化されるとして示されているが，もし演習 5.14 の方法を使うならこの代わりに $|0\rangle$ に初期化してもよい．この回路は 5.3.2 項で与えられる縮約を用いると素因数分解にも使える．

**演習 5.14:** 位数発見アルゴリズムで作られる量子状態は，もし第 2 レジスタを $|1\rangle$ に初期化すれば Fourier 逆変換の前において

$$|\psi\rangle = \sum_{j=0}^{2^t-1} |j\rangle U^j|1\rangle = \sum_{j=0}^{2^t-1} |j\rangle|x^j \bmod N\rangle \tag{5.46}$$

となる．もしも $U^j$ の代わりに

$$V|j\rangle|k\rangle = |j\rangle|k + x^j \bmod N\rangle \tag{5.47}$$

を計算する**異なる**ユニタリー変換 $V$ を用いて，第 2 レジスタの始状態を $|0\rangle$ とすると同じ状態が得られることを示せ．また $O(L^3)$ 個のゲートを用いて $V$ を構築する方法を示せ．

**連分数展開**

位数発見から位相推定への縮約は，位相推定アルゴリズムの結果 $\varphi \approx s/r$ から所望の答 $r$ を得る方法で完成する．我々は $\varphi$ を $2L+1$ ビット精度で知っているが，その他に**有理数**— 2 つの有界な整数の比 — であることがあらかじめわかっており，$\varphi$ に最も近い分数を計算できれば $r$ が得られる．

注目すべきことにこのタスクを効率良くこなす**連分数アルゴリズム** (continued fractions algorithm) と呼ぶアルゴリズムが存在する．この働きの例をコラム 5.3 に示す．このアルゴリズムが我々の要求を満たす理由は次の定理にある．この定理の証明は付録 D に示す．

**定理 5.1:** $s/r$ が

$$\left|\frac{s}{r} - \varphi\right| \le \frac{1}{2r^2} \tag{5.48}$$

を満たす有理数であるとする．このとき $s/r$ は $\varphi$ に対する連分数の収束値であり，連分数アルゴリズムを使って $O(L^3)$ 回の演算で計算できる．

$\varphi$ は $2L+1$ ビット精度を有する $s/r$ の近似値なので，$r \le N \le 2^L$ より $|s/r-\varphi| \le 2^{-2L-1} \le 1/2r^2$ が導ける．したがってこの定理が適用できる．

まとめると，$\varphi$ が与えられると連分数アルゴリズムにより $s'/r' = s/r$ となるような共通の公約数を持たない数 $s'$ と $r'$ が**効率良く**得られる．この数 $r'$ が求める位数の候補である．これが求める位数かどうかは，$x^{r'} \bmod N$ を計算して結果が 1 であるかどうかをみるとチェックできる．もしそうならば $r'$ は $N$ を法とする $x$ の位数であり，これが答である！

**コラム 5.3: 連分数アルゴリズム**

連分数とは次の形の表現を使って実数を整数だけで記述することである．

$$[a_0, \ldots, a_M] \equiv a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cdots + \frac{1}{a_M}}}}, \tag{5.49}$$

ここで $a_0, \ldots, a_M$ は正の整数である．（量子計算に応用するときは $a_0 = 0$ としたほうが便利である．）この連分数に対する $m$ **番目の収束値** ($m$-th convergent) を $[a_0, \ldots, a_m]$ ($0 \le m \le M$) と定義する．**連分数アルゴリズム** (continued fractions algorithm) は任意の実数の連分数展開を求める方法である．例を示すと容易にわかる．31/13 を連分数に分解するとしよう．連分数アルゴリズムの最初のステップでは 31/13 を整数部分と分数部分に分ける．

$$\frac{31}{13} = 2 + \frac{5}{13}. \tag{5.50}$$

次に分数部分を反転すると

$$\frac{31}{13} = 2 + \frac{1}{\frac{13}{5}}. \tag{5.51}$$

分離と反転プロセスを 13/5 に適用すると

$$\frac{31}{13} = 2 + \frac{1}{2 + \frac{3}{5}} = 2 + \frac{1}{2 + \frac{1}{\frac{5}{3}}}. \tag{5.52}$$

5/3 を分離・反転すると：

$$\frac{31}{13} = 2 + \frac{1}{2 + \frac{1}{1+\frac{2}{3}}} = 2 + \frac{1}{2 + \frac{1}{1+\frac{1}{\frac{3}{2}}}}. \tag{5.53}$$

ここで

$$\frac{3}{2} = 1 + \frac{1}{2} \tag{5.54}$$

は分子が 1 となってもはや反転する必要がないので連分数分解はここで終わり，31/13 の連分数展開の最終結果は

$$\frac{31}{13} = 2 + \frac{1}{2 + \frac{1}{1+\frac{1}{1+\frac{1}{2}}}}. \tag{5.55}$$

連分数アルゴリズムは現れる分子（上の例では 31, 5, 3, 2, 1）が確実に減少するので任意の有理数に対して有限回の「分離と反転」で終了する．どれくらい早く終るか？ もし $\varphi = s/r$ が有理数で $s$ と $r$ が $L$ ビットの整数ならば，$\varphi$ に対する連分数展開は — $O(L)$ 回の「分離と反転」，各回の計算に $O(L^2)$ 個のゲートを使って — $O(L^3)$ 回の演算で計算できる．

## 性　能

位数発見アルゴリズムが失敗するのはどんなときか？ これには 2 つの可能性がある．1 つは位相推定手続きが $s/r$ の誤った推定を下す場合である．これが起きる確率は最悪で $\epsilon$ であり，回路規模を僅か増やせばこれは小さくできる．もっと深刻なのは $r$ と $s$ が共通の因数を持つ場合であり，連分数アルゴリズムから返ってくる数 $r'$ は $r$ の因数であって $r$ そのものではない．幸いなことにこの問題には少なくとも 3 つの救い方がある．

最も直接的方法は 0 と $r-1$ の間でランダムに選んだ $s$ に対して，実際上 $s$ と $r$ が互いに素であることが多いのに留意することである．この場合，連分数アル

ゴリズムが $r$ を返してくる．これをみるには，問題 D.1 によると $r$ より小さい素数の数は少なくとも $r/2\log r$ であり，したがって，$s$ が素数（したがって $r$ と互いに素）である確率は少なくとも $1/2\log(r) > 1/2\log(N)$ である．したがって，アルゴリズムを $2\log(N)$ 回繰り返すと高い確率で $s$ と $r$ が互いに素である位相 $s/r$ を測定できて，連分数アルゴリズムで望み通りの $r$ が得られる．

第 2 の方法はもし $r' \neq r$ ならば $s = 0$ でない限り，$r'$ が $r$ の因数となる可能性の確率が $1/r \leq 1/2$ であることが保証されており，数回繰り返すとさらに減少する．$a$ を $a' \equiv a^{r'} (\text{mod } N)$ で置き換えるとする．このとき $a'$ の位数は $r/r'$ である．ここでアルゴリズムを繰り返して $a'$ の位数を計算すると，$r = r' \times r/r'$ なのでうまくいけば $a$ の位数が求められる．もし失敗すれば $r/r'$ の因子である $r''$ を得て，$a'' \equiv (a')^{r''} (\text{mod } N)$ の位数を計算する．この手続きを $a$ の位数が決定するまで繰り返す．各手続き毎にそのときの候補 $a^{''}\cdots$ の位数が少なくとも因子 2 だけ減少するので，必要な繰り返し数はたかだか $\log(r) = O(L)$ 回である．

第 3 の方法は $O(L)$ 回の試行でなくて一定回数の試行だけで済むので，前の 2 つより優れている．その考え方は位相推定・連分数展開の手続きを 2 回繰り返し，1 回目に $r'_1, s'_1$，2 回目に $r'_2, s'_2$ を得る．$s'_1$ と $s'_2$ が公約数を持たない場合には $r'_1$ と $r'_2$ の最小公倍数をとることにより $r$ が取り出せる．$s'_1$ と $s'_2$ が公約数を持たない確率は

$$1 - \sum_q p(q|s'_1)p(q|s'_2) \tag{5.56}$$

で与えられる．ここで総和は全素数 $q$ について行い，ここでの $p(x|y)$ は $y$ を整除する $x$ の確率を意味する．もし $q$ が $s'_1$ を整除するならば $s$ の真の値である 1 回目に得た $s_1$ も整除できて，上界 $p(q|s'_1)$ に対して $p(q|s_1)$ を上界とすれば十分である．ここで $s_1$ は 0 から $r-1$ の間で一様かつランダムに選ぶ．$p(q|s_1) \leq 1/q$，したがって $p(q|s'_1) \leq 1/q$ であることが容易にわかる．同様に $p(q|s'_2) \leq 1/q$ なので，$s'_1$ と $s'_2$ が公約数を持たない確率は次式を満たす：

$$1 - \sum_q p(q|s'_1)p(q|s'_2) \geq 1 - \sum_q \frac{1}{q^2}. \tag{5.57}$$

右辺の上界は幾つかの方法で求められる．簡単なテクニックが演習 5.16 に示されており，それによれば

$$1 - \sum_q p(q|s'_1)p(q|s'_2) \geq \frac{1}{4}. \tag{5.58}$$

したがって正しい $r$ を得る確率は少なくとも 1/4 である．

**演習 5.15:** 正の整数 $x$ と $y$ の最小公倍数は $xy/\gcd(x,y)$ であり，もし $x$ と $y$ が $L$ ビットの数ならば $O(L^2)$ 回の演算で計算できることを示せ．

**演習 5.16:** すべての $x \geq 2$ に対して $\int_x^{x+1} 1/y^2 dy \geq 2/3x^2$ を証明せよ．また

$$\sum_q \frac{1}{q^2} \leq \frac{3}{2}\int_2^\infty \frac{1}{y^2}dy = \frac{3}{4} \tag{5.59}$$

であり，したがって式 (5.58) が成立することを示せ．

このアルゴリズムはどれほどのリソースを消費するか？ Hadamard 変換にゲート $O(L)$ 個，Fourier 逆変換にゲート $O(L^2)$ 個が必要である．量子回路固有のコストは剰余指数化から生じていて，さらにゲート $O(L^3)$ 個を使用するので，量子回路固有の全ゲート数は $O(L^3)$ となる．連分数アルゴリズムにはさらに $O(L^3)$ のゲートが必要であり，$r'$ を得るには都合 $O(L^3)$ 個のゲートが必要である．$r'$ から $r$ を得る第 3 の方法では位数 $r$ を得るのに全コスト $O(L^3)$ でこの手続きを定数回繰り返すだけである．アルゴリズムを次にまとめておく．

**アルゴリズム：量子位数発見**

**入力：** (1) $L$ ビットの数と $N$ と互いに素な $x$ に対して，変換 $|j\rangle|k\rangle \rightarrow |j\rangle|x^j k \bmod N\rangle$ を実行するブラックボックス $U_{x,N}$.
(2) $|0\rangle$ に初期化された $t = 2L + 1 + \lceil \log(3 + \frac{1}{2\epsilon}) \rceil$ 個の q ビット．
(3) 状態 $|1\rangle$ に初期化された $L$ 個の q ビット．

**出力：** $x^r = 1 \pmod N$ を満たす最小の整数 $r > 0$.

**演算回数：** $O(L^3)$ 回の演算．成功確率 $O(1)$.

**手続き：**

**1.** $|0\rangle|1\rangle$ 　　初期状態

**2.** $\rightarrow \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} |j\rangle|1\rangle$ 　　重ね合せ

$$\mathbf{3}.\quad \to \frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}|j\rangle|x^j \bmod N\rangle \qquad U_{x,N}\text{を適用}$$

$$\approx \frac{1}{\sqrt{r2^t}}\sum_{s=0}^{r-1}\sum_{j=0}^{2^t-1}e^{2\pi isj/r}|j\rangle|u_s\rangle$$

$$\mathbf{4}.\quad \to \frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}|\widetilde{s/r}\rangle|u_s\rangle \qquad \text{第 1 レジスタに Fourier 逆変換を適用}$$

$$\mathbf{5}.\quad \to \widetilde{s/r} \qquad \text{第 1 レジスタを測定}$$

$$\mathbf{6}.\quad \to r \qquad \text{連分数アルゴリズムを適用}$$

### 5.3.2 応用：素因数分解

> 合成数と素数を見分ける問題と合成数を素数因子に分解する問題は数論の中で最も重要かつ有用なものである．... 科学の権威を保つにはそのように簡潔で高名な問題の解決を熱心に進めなければならない．
> — Carl Friedrich Gauss，Donald Knuth による引用．

正の合成数 $N$ が与えられたとき，どのような素数を掛け合わせるとそれに等しくなるか？この**素因数分解問題** (factoring problem) は，位数発見の高速アルゴリズムが容易に素因数分解の高速アルゴリズムに変換できるという意味で，いま述べた位数発見問題と等価であることがわかる．本項では素因数分解を位数発見に縮約する方法を説明し，この縮約の簡単な例を示す．

素因数分解を位数発見に縮約する手順は 2 つの基本的段階で進める．最初の段階で，もし方程式 $x^2 = 1 \pmod N$ の有意な解 $x \neq \pm 1 \pmod N$ が見い出せれば，$N$ の素因数が計算できることを示す．第 2 段階では $N$ と互いに素でランダムに選んだ $y$ は，$y^{r/2} \neq \pm 1 (\bmod\ N)$ を満たす偶数の位数 $r$ を有することが多く，したがって $x \equiv y^{r/2} (\bmod\ N)$ が $x^2 = 1 (\bmod\ N)$ の有意な解であるであることを示す．これら 2 つの段階は次の定理によって具体化されており，その証明は付録 D の D.3 節で示す．

**定理 5.2:** $N$ は $L$ ビットの合成数であり，$x$ は $1 \leq x \leq N$ の範囲で方程式 $x^2 = 1 \pmod N$ の自明でない解とする．つまり $x = 1 \pmod N$ でも

$x = N - 1 = -1 \pmod N$ でもないとする．このとき $\gcd(x-1,\ N)$ と $\gcd(x+1,\ N)$ の少なくとも一方が $N$ の有意な素因数であり，$O(L^3)$ 回の演算で計算できる．

**定理 5.3:** $N = p_1^{\alpha_1} \ldots p_m^{\alpha_m}$ は奇で正の合成数の素因数分解であるとする．$x$ は $1 \le x \le N-1$ の範囲から一様かつランダムに選んだ整数で，$N$ と互いに素であるとする．$r$ は $N$ を法とする $x$ の位数とする．このとき

$$p(r \text{ が偶数，かつ } x^{r/2} \neq -1 \pmod N) \ge 1 - \frac{1}{2^{m-1}}. \tag{5.60}$$

定理 5.2 と定理 5.3 を組み合わせると，任意の合成数 $N$ の有意な素因数を高い確率で返すアルゴリズムが得られる．このアルゴリズムの全ステップは（今日わかっている限り）アルゴリズムに使う位数発見「サブルーチン」を除いて，古典コンピュータで効率良く実行できる．この手続きを繰り返すと $N$ の完全な素因数分解が行える．そのアルゴリズムを以下に示す．

**アルゴリズム：素因数分解を位数発見に縮約**

**入力：**　合成数 $N$ .

**出力：**　$N$ の有意な素因数.

**所要時間：**　$O((\log N)^3)$ 回の演算．成功確率 $O(1)$ .

**手続き：**

1. もし $N$ が偶数ならば，素因数 2 を返す．
2. 整数 $a \ge 1$ と $b \ge 2$ に対して $N = a^b$ かどうかを決定し，もしそうならば素因数 $a$ を返す（演習 5.17 の古典アルゴリズムを使う）．
3. 1 から $N-1$ の範囲の $x$ をランダムに選ぶ．もし $\gcd(x,\ N) > 1$ ならば素因数 $\gcd(x,\ N)$ を返す．
4. $N$ を法とする $x$ の位数 $r$ を見出す位数発見サブルーチンを使う．
5. もし $r$ が偶数で $x^{r/2} \neq -1 \pmod N$ ならば $\gcd(x^{r/2}-1,\ N)$ と $\gcd(x^{r/2}+1,\ N)$ を計算し，これらの 1 つが有意な素因数であることを試して，そうならばその素因数を返す．そうでなければアルゴリズムは成立しない．

このアルゴリズムのステップ 1 と 2 は素因数を返すか，そうでなければ $N$ が奇数の整数で 1 つ以上の素因数を持つことを確認する．これらのステップはそれぞれ $O(1)$ と $O(L^3)$ で実行できる．ステップ 3 では素因数を返すか，$\{0,1,2,\ldots,N-1\}$ からランダムに選んだ要素 $x$ を返す．ステップ 4 では位数発見サブルーチンを呼び出して，$N$ を法とする $x$ の位数 $r$ を計算する．定理 5.3 により少なくとも 1/2 の確率で $r$ が偶数であって $x^{r/2} \neq -1 (\mathrm{mod}\ N)$ であることが保証されており，次に定理 5.2 により $\gcd(x^{r/2}-1,\ N)$ または $\gcd(x^{r/2}+1,\ N)$ が $N$ の有意な素因数であることが保証されているので，ステップ 5 でアルゴリズムが完了する．量子位数発見サブルーチンを使ったこのアルゴリズムの用法例をコラム 5.4 に示す．

**コラム 5.4: 量子力学的な 15 の素因数分解**

量子素因数分解アルゴリズムにおける位数発見，位相推定および連分数展開の用例として，$N=15$ の素因数分解への適用例を示す．最初に $N$ と共通因数を持たないランダムな数を選ぶ．例えば $x=7$ とする．次に量子位数発見アルゴリズムを使って $N$ に関する $x$ の位数を計算する：状態 $|0\rangle|0\rangle$ から始めて，第 1 レジスタに $t=11$ の Hadamard 変換を適用して状態

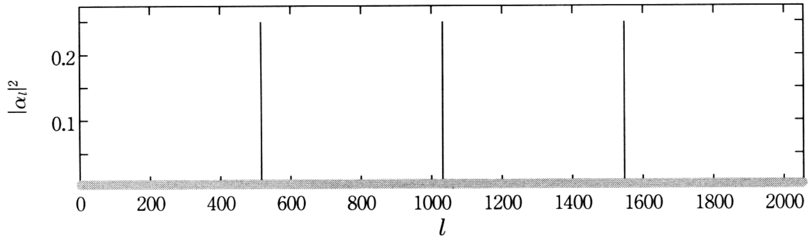
$$\frac{1}{\sqrt{2^t}}\sum_{k=0}^{2^t-1}|k\rangle|0\rangle = \frac{1}{\sqrt{2^t}}\left[|0\rangle+|1\rangle+|2\rangle\cdots|2^t-1\rangle\right]|0\rangle \tag{5.61}$$

を作る．$t$ をこの値に選ぶと誤り確率 $\epsilon$ はたかだか 1/4 であることが保証される．次に $f(x)=x^k \bmod N$ を計算し結果を第 2 レジスタに渡す：

$$\begin{aligned}&\frac{1}{\sqrt{2^t}}\sum_{k=0}^{2^t-1}|k\rangle|x^k \bmod N\rangle\\ &= \frac{1}{\sqrt{2^t}}\left[|0\rangle|1\rangle+|1\rangle|7\rangle+|2\rangle|4\rangle+|3\rangle|13\rangle+|4\rangle|1\rangle+|5\rangle|7\rangle+|6\rangle|4\rangle+\cdots\right].\end{aligned} \tag{5.62}$$

第 1 レジスタに Fourier 逆変換 $FT^\dagger$ を実行してそれを測定する．得られた出力分布を解析する 1 つの方法は，第 1 レジスタの縮約した密度行列を計算し，$FT^\dagger$ を適用して測定統計を計算する．しかし第 2 レジスタにはこれ以上の演算は実行しないので，代わりに暗黙測定の原理（4.4 節）を適用して第 2 レジスタを測

定すると仮定して，1, 7, 4, 13 の中から**ランダム**に結果を選ぶ．（他の結果でもよいが）4 を選ぶとこれは $FT^\dagger$ への入力が $\sqrt{\frac{4}{2^t}}[|2\rangle+|6\rangle+|10\rangle+|14\rangle+\cdots]$ であったことを意味する．$FT^\dagger$ を適用するとある状態 $\sum_l \alpha_l|l\rangle$ が得られる．$2^t = 2048$ に対する確率分布 $|\alpha_l|^2$ を図に示す．




したがって，最終測定で $0, 512, 1024$, または 1536 が得られ，それぞれの確率は正確に 1/4 である．いま測定により $l = 1536$ を得たとして，連分数展開を計算すると $1536/2024 = 1/(1+(1/3))$，したがって展開の収束値として 3/4 が得られ，$x = 7$ の位数として $r = 4$ を得る．たまたま $r$ が偶数でさらに $x^{r/2} \bmod N = 7^2 \bmod 15 = 4 \neq -1 \bmod 15$ なのでアルゴリズムは成立し，最大公約数 $\gcd(x^2-1,\ 15) = 3$ と $\gcd(x^2+1,\ 15) = 5$ から $15 = 3 \times 5$ がわかる．

**演習 5.17:** $N$ は $L$ ビット長とする．この演習の目的は，ある整数 $a \geq 1$ と $b \geq 2$ に対して $N = a^b$ であるかどうかを決定する効率の良い古典アルゴリズムを見つけることである．これは次のよう行う．

(1) もし $b$ が存在するならば，$b \leq L$ を満たすことを示せ．

(2) $\log_2 N$，$b \leq L$ に対する $x = y/b$，および $2^x$ に最も近い 2 つの整数 $u_1$ と $u_2$ を計算するのに，たかだか $O(L^2)$ 回の演算を必要とすることを示せ．

(3) $u_1^b$ と $u_2^b$ を計算し（2 乗を繰り返せ），そのいずれかが $N$ に等しいかどうかを確かめるのに，たかだか $O(L^2)$ 回の演算を要することを示せ．

(4) 前の結果を組み合わせて，整数 $a$ と $b$ に対して $N = a^b$ が成り立つかどうかを決めるための $O(L^3)$ 回の演算を要するアルゴリズムを与えよ．

**演習 5.18:（91 の素因数分解）** $N = 91$ の素因数分解を行うとする．ステップ 1 と 2 が成り立つことを確かめよ．ステップ 3 に対して，91 と互いに素な $x = 4$ を選ぶとする．$N$ に関する $x$ の位数 $r$ を計算し，$x^{r/2} \bmod 91 = 64 \neq -1 \pmod{91}$ なのでアルゴリズムは成功し $\gcd(64-1,\ 91) = 7$ を与えることを示せ．

この方法は 91 の素因数分解に対する最も効率の良い方法ではなさそうである．実際もしすべての計算を古典コンピュータで行うならば，古典コンピュータ上で位数発見問題を解く効率的方法が知られていないので，この縮約によって効率の良い素因数分解アルゴリズムが得られたことにはならないであろう．

**演習 5.19:** 位数発見サブルーチンが必要とされる最小の数が $N = 15$ であること，つまり偶数でなく何か小さい数のベキでもない最小の合成数であることを示せ．

## 5.4　量子 Fourier 変換の一般的応用

本章でこれまでに述べてきた量子 Fourier 変換の主要な応用は位相推定と位数発見である．これらのテクニックを使って他にどんな問題が解けるか？ 本節では**隠れ部分群問題** (hidden subgroup problem) と呼ぶ非常に一般的問題を取り扱い，それを解く効率的量子アルゴリズムについて述べる．この問題はわかっているすべての量子 Fourier 変換の「指数関数的に速い」応用を含んでおり，関数の領域と範囲が非常に複雑な構造を有する状況で周期関数の未知周期を見出すタスクを一般化したものと考えられる．最も扱い易い形で問題を提示するために，2 つの特殊な応用 ―（1 次元関数の）周期発見と離散対数 ― から始める．その次に一般の隠れ部分群問題に向かう．本節の内容は本章の他の節に比べてどちらかというと概略的で概念的なので，必然的にすべて詳細を理解しようとする読者には一層の努力が求められる！

### 5.4.1 周期発見

次の問題を考える．$f$ はある未知の $0 \le r \le 2^L$ に対して，単一ビットを出力し $f(x+r) = f(x)$ を満たす周期関数であるとする．ただし $x$，$r \in \{0, 1, 2, \ldots\}$ である．ユニタリー変換 $U|x\rangle|y\rangle \to |x\rangle|y \oplus f(x)\rangle$（$\oplus$ は 2 を法とする和）を行う量子ブラックボックス $U$ が与えられると，$r$ を決定するには幾回のブラックボックス質問 (query) とその他の演算が必要か？ 実際に $U$ は有限領域に作用し，領域のサイズは $r$ に対する要求精度で決まることに注意する．次に示すのはこの問題を **1 回**の質問と $O(L^2)$ 回の他の演算を用いて解く量子アルゴリズムである．

**アルゴリズム：周期発見**

**入力：** (1) $U|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$ を実行するブラックボックス．
(2) 関数評価を蓄積する状態，$|0\rangle$ に初期化．
(3) $|0\rangle$ に初期化された $t = O(L + \log(1/\epsilon))$ 個の q ビット．

**出力：** $f(x+r) = f(x)$ なる最小の整数 $r > 0$.

**演算回数：** $U$ を 1 回使用，$O(L^2)$ 回の演算．成功確率は $O(1)$.

**手続き：**

**1.** $|0\rangle|0\rangle$ 　　初期状態

**2.** $$\to \frac{1}{\sqrt{2^t}} \sum_{x=0}^{2^t-1} |x\rangle|0\rangle$$ 　　重ね合せ

**3.** $$\to \frac{1}{\sqrt{2^t}} \sum_{x=0}^{2^t-1} |x\rangle|f(x)\rangle$$ 　　$U$ を適用

$$\approx \frac{1}{\sqrt{r2^t}} \sum_{l=0}^{r-1} \sum_{x=0}^{2^t-1} e^{2\pi i l x/r}|x\rangle|\hat{f}(l)\rangle$$

**4.** $$\to \frac{1}{\sqrt{r}} \sum_{l=0}^{r-1} |\widetilde{l/r}\rangle|\hat{f}(l)\rangle$$ 　　第1レジスタに Fourier 逆変換を適用

**5.** $\to \widetilde{l/r}$ 　　第1レジスタを測定

**6.** $\to r$ 　　連分数アルゴリズムを適用

このアルゴリズムは量子位数発見とほぼ同じであり，位相推定に基づいている
このアルゴリズムを理解する鍵はステップ 3 にある．ここで $|f(x)\rangle$ の Fourier 変換である状態：

$$|\hat{f}(l)\rangle \equiv \frac{1}{\sqrt{r}} \sum_{x=0}^{r-1} e^{-2\pi i l x/r} |f(x)\rangle \tag{5.63}$$

を導入している．ステップ 3 の等式は次式を使っている．

$$|f(x)\rangle = \frac{1}{\sqrt{r}} \sum_{l=0}^{r-1} e^{2\pi i l x/r} |\hat{f}(l)\rangle. \tag{5.64}$$

この式は $x$ が $r$ の整数倍のときに $\sum_{l=0}^{r-1} e^{2\pi i l x} = r$，その他は 0 であることに留意すると容易に証明できる．ステップ 3 の近似等号は一般に $2^t$ が必ずしも $r$ の整数倍ではない（これは必ずしも必要ではなく，位相推定限界により考慮されている）ので必要である．ステップ 4 で第 1 レジスタに Fourier 逆変換式 (5.22) を適用すると，位相 $l/r$ の推定値が得られる．ここで $l$ はランダムに選ばれる．最後のステップで連分数展開により $r$ が効率良く得られる．

なぜこれがうまく働くのか？ それを理解する 1 つの方法は式 (5.63) が $\{0, 1, \ldots, 2^L - 1\}$ における $|f(x)\rangle$ の Fourier 変換を近似することと（演習 5.20 参照），コラム 5.5 で述べるように Fourier 変換が持つ**シフト不変性** (shift invariance) と呼ぶ非常に便利で興味ある性質を理解することである．もう 1 つ理解すべきことは位数発見アルゴリズムが実行するのは関数 $f(x) = x^k \bmod N$ の周期を見出すことだけであり，一般の周期関数の周期を見出すことは期待されていない．もう 1 つ別の理解の方法は演習 5.21 で述べるように，固有ベクトルが正確に $|\hat{f}(l)\rangle$ であるユニタリーオペレータを使うと，ブラックボックス $U$ が自然に実行されて，5.2 節の位相推定手続きが適用できることである．

### コラム 5.5: Fourier 変換のシフト不変性

Fourier 変換 (5.1) は**シフト不変性**と呼ぶ興味深くかつ非常に便利な性質を持っている．この性質の一般的応用を記述するのに便利な記号を使って，量子 Fourier 変換を記述すると

$$\sum_{h \in H} \alpha_h |h\rangle \rightarrow \sum_{g \in G} \tilde{\alpha}_g |g\rangle, \tag{5.65}$$

ここで $\tilde{\alpha}_g = \sum_{h\in H} \alpha_h \exp(2\pi igh/|G|)$，$H$ は $G$ のある部分集合，$G$ は Hilbert 空間の正規直交基底にある状態の指数を表す．例えば $G$ は $n$ 個の q ビットシステムに対する 0 から $2^n - 1$ の数の集合である．$|G|$ は $G$ の要素の数を表す．初期状態に次のユニタリー変換を実行するオペレータ $U_k$ を適用しその後に Fourier 変換を行う．

$$U_k|g\rangle = |g+k\rangle. \tag{5.66}$$

この結果

$$U_k \sum_{h\in H} \alpha_h|h\rangle = \sum_{h\in H} \alpha_h|h+k\rangle \to \sum_{g\in G} e^{2\pi igk/|G|}\tilde{\alpha}_g|g\rangle \tag{5.67}$$

は $|g\rangle$ の振幅の大きさが $k$ によらず変化しない，つまり $|\exp(2\pi igk/|G|)\tilde{\alpha}_g| = |\tilde{\alpha}_g|$ という性質を持つ．

群論の用語では $G$ は群，$H$ は $G$ の部分群であって，もし $G$ 上の関数 $f$ が $H$ の剰余類 (coset) 上で一定ならば，$f$ の Fourier 変換は $H$ の剰余類上で不変であるという．

**演習 5.20:** $r$ の整数倍である $N$ に対して，$f(x+r) = f(x)$, $0 \le x \le N$ とする．次式を計算してその結果と式 (5.63) の関係を示せ．

$$\hat{f}(l) \equiv \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} e^{-2\pi ilx/N} f(x). \tag{5.68}$$

このとき次の事実が必要になろう．

$$\sum_{k\in\{0,r,2r,\dots,N-r\}} e^{2\pi ikl/N} = \begin{cases} N/r, & l \text{ が } N/r \text{ の整数倍のとき} \\ 0, & \text{その他のとき} \end{cases} \tag{5.69}$$

**演習 5.21:（周期発見と位相推定）** 上で述べた周期関数に対し変換 $U_y|f(x)\rangle = |f(x+y)\rangle$ を実行するユニタリーオペレータ $U_y$ が与えられたとする．

(1) $U_y$ の固有ベクトルが $|\hat{f}(l)\rangle$ であることを示しその固有値を求めよ．

(2) ある $x_0$ に対して $|f(x_0)\rangle$ が与えられたとき，周期発見問題を解くのに，$U$ と同様に有用なブラックボックスを $U_y$ を使って実現できることを示せ．

### 5.4.2 離散対数

いま考えた周期発見問題は周期関数の定義域 (domain) と値域 (range) が整数であるという簡単なものであった．関数がもう少し複雑になるとどうなるか？ 関数 $F(x_1,\ x_2) = a^{sx_1+x_2} \mathrm{mod}\ N$ を考える．ここで全変数は整数, $r$ は $a^r \bmod N = 1$ なる最小の正の整数である．この関数は $f(x_1+l,\ x_2-ls) = f(x_1,\ x_2)$ なので周期的であるが, 周期は整数 $l$ に対して 2 項組 (2-tuple) $(l,\ ls)$ である．これは奇妙な関数に見えるかも知れないが, $s$ を決定する**離散対数**問題— $a$ と $b = a^s$ が与えられたときに $s$ は何か？ — と呼ばれる問題を解くことができるので, 暗号において非常に有用である．この問題はユニタリー変換 $U|x_1\rangle|x_2\rangle|y\rangle \to |x_1\rangle|x_2\rangle|y \oplus f(x)\rangle$（$\oplus$ はビット毎の 2 を法とする和）を実行するブラックボックス $U$ の **1** つの質問と, $O(\lceil \log r \rceil^2)$ 回の他の演算を使う量子アルゴリズムで解くことができる．$a^r \bmod N = 1$ なる最小の $r > 0$ が既知であるという仮定が必要があるが, これは前述の位数発見アルゴリズムを用いて得られる．

**アルゴリズム：離散対数**

**入力：** (1) $f(x_1, x_2) = b^{x_1} a^{x_2}$ に対して演算

$$U|x_1\rangle|x_2\rangle|y\rangle = |x_1\rangle|x_2\rangle|y \oplus f(x_1, x_2)\rangle$$

を実行するブラックボックス．

(2) 関数評価を蓄積する状態, $|0\rangle$ に初期化．

(3) $t = O(\lceil \log r \rceil + \log(1/\epsilon))$ 個の q ビットを収容するレジスタ 2 個, $|0\rangle$ に初期化．

**出力：** $a^s = b$ なる最小の正の整数 $s$.

**演算回数：** $U$ を 1 回使用, および $O(\lceil \log r \rceil)$ 回の演算．成功確率は $O(1)$.

**手続き：**

**1**. $|0\rangle|0\rangle|0\rangle$ 　　初期化

**2**. $\to \frac{1}{2^t} \sum_{x_1=0}^{2^t-1} \sum_{x_2=0}^{2^t-1} |x_1\rangle|x_2\rangle|0\rangle$ 　　重ね合せを作成

**3.** $\rightarrow \frac{1}{2^t}\sum_{x_1=0}^{2^t-1}\sum_{x_2=0}^{2^t-1}|x_1\rangle|x_2\rangle|f(x_1,x_2)\rangle$　$U$ を適用

$$\approx \frac{1}{2^t\sqrt{r}}\sum_{l_2=0}^{r-1}\sum_{x_1=0}^{2^t-1}\sum_{x_2=0}^{2^t-1} e^{2\pi i(sl_2x_1+l_2x_2)/r}|x_1\rangle|x_2\rangle|\hat{f}(sl_2,l_2)\rangle$$

$$= \frac{1}{2^t\sqrt{r}}\sum_{l_2=0}^{r-1}\left[\sum_{x_1=0}^{2^t-1} e^{2\pi i(sl_2x_1)/r}|x_1\rangle\right]\left[\sum_{x_2=0}^{2^t-1} e^{2\pi i(l_2x_2)/r}|x_2\rangle\right]$$
$$|\hat{f}(sl_2,l_2)\rangle$$

**4.** $\rightarrow \frac{1}{\sqrt{r}}\sum_{l_2=0}^{r-1}|\widetilde{sl_2/r}\rangle|\widetilde{l_2/r}\rangle|\hat{f}(sl_2,l_2)\rangle$　最初の 2 レジスタに Fourier 逆変換を適用

**5.** $\rightarrow (\widetilde{sl_2/r},\widetilde{l_2/r})$　最初の 2 レジスタを測定

**6.** $\rightarrow s$　一般化した連分数アルゴリズムを適用

ここでもこのアルゴリズムを理解する鍵はステップ 3 にあり，$|f(x_1,x_2)\rangle$ の Fourier 変換として状態：

$$|\hat{f}(l_1,l_2)\rangle = \frac{1}{\sqrt{r}}\sum_{j=0}^{r-1} e^{-2\pi i l_2 j/r}|f(0,j)\rangle \tag{5.70}$$

を導入している（演習 5.22 参照）．この式で $l_1$ と $l_2$ の値は次式を満たさねばならない：

$$\sum_{k=0}^{r-1} e^{2\pi i k(l_1/s-l_2)/r} = r. \tag{5.71}$$

そうでなければ $|\hat{f}(l_1,\ l_2)\rangle$ の振幅はほぼ 0 である．$s$ を決める最後のステップで使う一般化した連分数展開は 5.3.1 項で使った手続きと同様であり，その構築は簡単な演習として残しておく．

**演習 5.22:** 次式が成立することを示せ．また，この式が 0 でないためには $l_1/s-l_2$ が $r$ の整数倍に制約されることを示せ．

$$|\hat{f}(l_1,\ l_2)\rangle = \sum_{x_1=0}^{r-1}\sum_{x_2=0}^{r-1} e^{2\pi i(l_1x_1+l_2x_2)/r}|f(x_1,\ x_2)\rangle$$
$$= \frac{1}{\sqrt{r}}\sum_{j=0}^{r-1} e^{-2\pi i l_2 j/r}|f(0,\ j)\rangle. \tag{5.72}$$

**演習 5.23:** 式 (5.70) を用いて次式を計算し，結果が $f(x_1, x_2)$ であることを示せ．

$$\frac{1}{r}\sum_{l_1=0}^{r-1}\sum_{l_2=0}^{r-1} e^{-2\pi i(l_1x_1+l_2x_2)/r}|\hat{f}(l_1, l_2)\rangle. \tag{5.73}$$

**演習 5.24:** 離散対数アルゴリズムのステップ **6** で，$sl_2/r$ と $l_2/r$ の推定値から $s$ を決定するに必要な，一般化した連分数アルゴリズムを構築せよ．

**演習 5.25:** パラメータ $a$ と $b$ を取り入れて，ユニタリー変換 $|x_1\rangle|x_2\rangle|y\rangle \rightarrow |x_1\rangle|x_2\rangle|y \oplus b^{x_1}a^{x_2}\rangle$ を実行する，ブラックボックス $U$ に対する量子回路を構築せよ．この回路は量子離散対数アルゴリズムで用いられる．基本的演算が幾つ使われるか？

### 5.4.3 隠れ部分群問題

周期性構造が全く複雑な場合でも，周期関数が与えられると周期を効率的に決定する量子アルゴリズムが使えるという様式がこれまでに明らかになった．しかし重要なことは周期関数の**すべての**周期が決められるわけではない．この疑問に対する広い枠組みを定義する一般的問題は，群論の言葉で次のように簡潔に表現される（手早く復習するには付録 B 参照）：

> $f$ は有限に生成された群 $G$ から有限集合 $X$ への関数であり，部分群 $K$ の剰余類上で一定，各剰余類上で互いに異なるとする．$g \in G$, $h \in X$ および適切に選んだ $X$ への 2 進数演算 $\oplus$ に対して，ユニタリー変換 $U|g\rangle|h\rangle = |g\rangle|h \oplus f(g)\rangle$ を実行する量子ブラックボックスが与えられたとき，$K$ に対する生成集合を見出せ．

位数発見，周期発見，離散対数その他多くの問題はこの**隠れ部分群問題** (hidden subgroup problem) の事例であり，興味あるものを図 5.5 にまとめた．

| 名称 | G | X | K | 関数 |
|---|---|---|---|---|
| Deutsch | $\{0,\ 1\}, \oplus$ | $\{0,\ 1\}$ | $\{0\}$ または $\{0,\ 1\}$ | $K = \{0,\ 1\}$ : $\begin{cases} f(x) = 0 \\ f(x) = 1 \end{cases}$ $K = \{0\}$ : $\begin{cases} f(x) = x \\ f(x) = 1 - x \end{cases}$ |
| Simon | $\{0,\ 1\}^n, \oplus$ | 任意の有限集合 | $\{0,\ s\}$ $s \in \{0,\ 1\}^n$ | $f(x \oplus s) = f(x)$ |
| 周期発見 | $\mathbf{Z},\ +$ | 任意の有限集合 | $\{0, r, 2r, \ldots\}$ $r \in G$ | $f(x + r) = f(x)$ |
| 位数発見 | $\mathbf{Z},\ +$ | $\{a^j\}$ $j \in Z_r$ $a^r = 1$ | $\{0, r, 2r, \ldots\}$ $r \in G$ | $f(x) = a^x$, $f(x + r) = f(x)$ |
| 離散対数 | $\mathbf{Z}_r \times \mathbf{Z}_r$ $+(\text{mod } r)$ | $\{a^j\}$ $j \in Z_r$ $a^r = 1$ | $(l,\ -ls)$ $l,\ s \in \mathbf{Z}_r$ | $f(x_1,\ x_2) = a^{kx_1 + x_2}$; $f(x_1 + l,\ x_2 - ls)$ $= f(x_1,\ x_2)$ |
| 置換の位数 | $\mathbf{Z}_{2^m} \times \mathbf{Z}_{2^n}$ $+(\text{mod} 2^m)$ | $\mathbf{Z}_{2^n}$ | $\{0, r, 2r, \ldots\}$ $r \in X$ | $f(x, y) = \pi^x(y)$; $f(x + r, y) = f(x, y)$; $\pi = X$ の置換 |
| 隠れ線形関数 | $\mathbf{Z} \times \mathbf{Z},\ +$ | $\mathbf{Z}_N$ | $(l,\ -ls)$ $l,\ s \in X$ | $f(x_1,\ x_2)$ $= \pi(sx_1 + x_2 \text{ mod } N)$; $\pi = X$ の置換 |
| Abel の固定群 | $(H,\ X)$ $H =$ 任意の Abel 群 | 任意の有限集合 | $\{s \in H \mid$ $f(s,\ x) = x,$ $\forall x \in X\}$ | $f(gh,\ x)$ $= f(g,\ f(h,\ x))$; $f(gs,\ x) = f(g,\ x)$ |

**図 5.5:** 隠れ部分群問題．関数 $f$ は群 $G$ から有限集合 $X$ に写像し，隠れ部分群 $K \subseteq G$ の剰余類 (coset) 上で一定であることが約束されている．この表で $\mathbf{Z}_N$ は集合 $\{0,\ 1, \ldots, N-1\}$ を表し，$\mathbf{Z}$ は整数である．問題は $f$ に対するブラックボックスが与えられたときに $K$（または $K$ の生成集合）を見出すことである．

有限の **Abel 群** (Abelian group) $G$ に対して，量子コンピュータは本項で述べた他のアルゴリズムと非常に似た方法で，$\log |G|$ の多項式数の演算回数とブラックボックスによる関数評価を 1 回行うことにより，隠れ部分群問題を解くことが

できる．（実際には同様の方法で無限に生成された Abel 群に対する解も可能であるが，ここでは有限の場合に話を限る．）アルゴリズムの詳細設計は演習として読者に任せるが，基本的考え方の説明を読めば容易に解けるであろう．有限の Abel 群は剰余計算における整数に関する加法群の積と同形 (isomorphic) なので，大部分はこれまでと本質的に同じである．これは $G$ における $f$ の量子 Fourier 変換が定義されて（付録 B.3 節参照），効率良く実行できることを意味する．アルゴリズムの最初の有意なステップでは Fourier 変換を用いて（Hadamard 演算を一般化して）群の要素の重ね合せを作り，次のステップで $f$ に対する量子ブラックボックスを適用して重ね合せを変換して次式を得る．

$$\frac{1}{\sqrt{|G|}}\sum_{g\in G}|g\rangle|f(g)\rangle. \tag{5.74}$$

前と同じく $|f(g)\rangle$ を Fourier 基底で書き直す．出発点は，

$$|f(g)\rangle = \frac{1}{\sqrt{|G|}}\sum_{l=0}^{|G|-1} e^{2\pi i lg/|G|}|\hat{f}(l)\rangle, \tag{5.75}$$

ここで指数 $l$ を持つ $g\in G$ の表現（演習 B.13 参照）として $\exp[-2\pi i lg/|G|]$ を選んだ．（Fourier 変換は群の要素と表現の間の写像である．演習 B.23 参照．）$f$ は部分群 $K$ の剰余類上で一定で互いに異なるので，

$$|\hat{f}(l)\rangle = \frac{1}{\sqrt{|G|}}\sum_{g\in G} e^{-2\pi i lg/|G|}|f(g)\rangle \tag{5.76}$$

は

$$\sum_{h\in K} e^{-2\pi i lh/|G|} = |K| \tag{5.77}$$

を満たす $l$ 以外のすべての $l$ の値に対してほぼ 0 の振幅を有し，したがって式 (5.57) が簡単にできることを認識するのが要点である．もし $l$ が決定できれば，この式で与えられる線形の制約によって $K$ の要素を決めることができ，$K$ は Abel 群なので最終的に隠れ部分群全体に対する生成集合が決定できて，問題が解ける．

しかし世の中はそれほど簡単ではない．周期発見と離散対数がうまくいく理由は，連分数展開で $l/|G|$ から $l$ を得るのに成功するからである．これらの問題で

は $l$ と $|G|$ は高い確率で公約数を持たないようになっていた．しかし $|G|$ は自由な合成数なので一般にこれは成り立たないかも知れず，また $l$ についてあらかじめ役立つ情報も得られないはずである．

幸いこの問題は次のように解決できる．上述のように任意の Abel 群 $G$ は素数ベキ位数を有する巡回群の積と同形，つまり $G = \mathbf{Z}_{p_1} \times \mathbf{Z}_{p_2} \times \cdots \times \mathbf{Z}_{p_M}$ である．ここで $p_i$ は素数，$\mathbf{Z}_{p_i}$ は $p_i$ を法とする和を群の演算とする整数 $\{0, 1, \ldots, p_i - 1\}$ に関する群を表す．したがって式 (5.75) に現れる位相を書き直すと $g_i \in \mathbf{Z}_{p_i}$ に対して

$$e^{2\pi ilg/|G|} = \prod_{i=1}^{M} e^{2\pi il'_i g_i/p_i}. \tag{5.78}$$

今度は位相推定手続きによって $l'_i$ がわかり，これから $l$ が決定でき，したがって上に述べたように $K$ の要素が決まって隠れ部分群問題が解ける．

**演習 5.26:** $K$ は $G$ の部分群なので，$G$ を素数ベキ位数の巡回群の積に分解すると $K$ も分解される．式 (5.77) を書き直して，$l'_i$ を決めると対応する $K$ の巡回部分群 $K_{p_i}$ の要素が決まることを示せ．

**演習 5.27:** 一般の有限 Abel 群 $G$ を素数ベキ位数の巡回群の積に分解することは，もちろん通常困難な問題である（少なくとも例えば整数の素因数分解と同様に困難である）．ここで再び量子アルゴリズムの出番である： 本章のアルゴリズムを如何に使えば望み通りに $G$ を効率良く分解できるか説明せよ．

**演習 5.28:** 有限 Abel 群に対する隠れ部分群問題を解く量子アルゴリズムの詳細な仕様を書き下し，所要演算回数と成功確率を推定せよ．

**演習 5.29:** 図 5.5 に示した Deutsch の問題と Simon の問題を，隠れ部分群問題の枠組みを用いて解く量子アルゴリズムを示せ．

### 5.4.4　他の量子アルゴリズムは？

隠れ部分群問題に関する量子アルゴリズムを記述する枠組みにおいて，最も興味ある側面はいろいろな群 $G$ や関数 $f$ を考えることにより，もっと難しい問題が

解けるかも知れないと示唆している点である．我々が述べたのは Abel 群に対するこの問題の解だけである．非 Abel 群に対してはどうか？ これは非常に興味ある問題である（非 Abel 群における一般の Fourier 変換の議論は付録 B 参照）：例えば**グラフ同形** (graph isomorphism) 問題は，$n$ 個の頂点のラベルを並べ替えたときに与えられる 2 つのグラフが同じかどうかを決定する（3.2.3 項：第 I 巻）．これらの並べ替えは対称群 $S_n$ の変換で記述され，これらの群に対する高速 Fourier 変換を実行するアルゴリズムが存在する．しかしグラフ同形問題を効率的に解く量子アルゴリズムは知られていない．

隠れ部分群問題のより一般の場合は量子コンピュータで解けないとしても，如何にすれば限界の外に踏み出せるかという疑問が湧くので，この統一の枠組みを作ることは有益である．発見されるすべての高速量子アルゴリズムが隠れ部分群問題の解に通じるとは信じ難い．これらの問題が Fourier 変換の剰余類不変性に基礎を置いていると考えると，新たなアルゴリズムを探索する際になすべきことは，異なる不変性を持つ他の変換を調べることかも知れない．他の方向を目指すなら，任意の（しかし問題とは独立に規定された）量子状態が手助けとして与えられるならば，どのような困難な隠れ部分群問題が効率良く解けるか？という質問になるかも知れない．結局 4 章で議論したように，実際にたいていの量子状態を構築するのは指数関数的に困難である．そのような状態を使って量子アルゴリズムが困難な問題が解けるならば，それは有用なリソース（真の「量子オラクル」）となる！

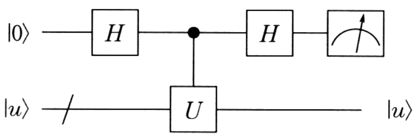
隠れ部分群問題はまた，次のような古典的に対応する問題に比べて指数関数的に高速な量子アルゴリズムに潜む重要な制約を明らかにする．それは「$F(X)$ はこれこれの性質を有することが約束されている．その性質の特徴を明らかにせよ」という形を意味する**約束問題** (promise problem) である．少しがっかりすることであるが，ある種の約束なしに問題を解くと量子コンピュータは古典コンピュータに比べて指数関数的高速化が**できず**，最大の高速化は多項式的であることを次章の最後に示す．他方これは量子コンピュータがどのような種類の問題に威力を発揮するかという，重要な手がかりを与えてくれる．振り返ってみると，隠れ部分群問題は量子計算の自然な候補であったと考えられるかも知れない．他にどんな自然な候補があるだろうか？ 考えてみよう！

**問題 5.1:** 次の量子 Fourier 変換を実行する量子回路を構築せよ．ここで $p$ は素数である．

$$|j\rangle \to \frac{1}{\sqrt{p}}\sum_{k=0}^{p-1} e^{2\pi ijk/p}|k\rangle \tag{5.79}$$

**問題 5.2:（量子 Fourier 変換の測定）** 量子計算の最終段階で量子 Fourier 変換を実行し，その後で計算基底による測定を行うとする．量子 Fourier 変換と測定の組み合わせは **1** - q ビットゲートと古典的制御を伴う測定だけで成り立つ回路と等価であり，2 - q ビットのゲートは必要ないことを示せ．4.4 節の議論が役に立つであろう．

**問題 5.3:（Kitaev のアルゴリズム）** 下図の量子回路を考える．ここで $|u\rangle$ は固有値 $e^{2\pi i\varphi}$ を有する $U$ の固有状態である．




上側の q ビットの測定値は確率 $p \equiv \cos^2(\pi\varphi)$ で 0 であることを示せ．$|u\rangle$ は回路によって影響されないので再利用が可能である．$k$ は任意に選べる整数として，$U$ を $U^k$ で置き換えることができるとすれば，この回路を繰り返して $k$ を適当に増やすことによって，望み通りの $p$ のビット — したがって $\varphi$ のビット — が効率良く得られることを示せ．これは位相推定アルゴリズムの代案である．

**問題 5.4:** 素因数分解アルゴリズムで与えた演算回数の上界 $O(L^3)$ はタイトではない．より良い上界として $O(L^2 \log L \log\log L)$ 回の演算で達成できることを示せ．

**問題 5.5:（非 Abel 群の隠れ部分群 — 研究）** $f$ は有限群 $G$ から任意の有限値域 $X$ への関数であり，さらに部分群 $K$ の異なる左剰余類上で一定かつ異なることが約束されているものとする．状態：

$$\frac{1}{\sqrt{|G|^m}}\sum_{g_1,\ldots,g_m}|g_1,\ldots,g_m\rangle|f(g_1),\ldots,f(g_m)\rangle \tag{5.80}$$

から出発して $m = 4\log|G| + 2$ を選ぶと，少なくとも $1 - 1/|G|$ の確率で $K$ を決めることができることを証明せよ．$G$ は必ずしも Abel 群である必要はなく，$G$ 上で Fourier 変換ができることも要求されていないことに注意する．この結果は（$O(\log|G|)$ 回のオラクル呼び出しを使って）異なる可能な隠れ部分群に対応する純粋状態出力がほぼ直交するような，最終結果が得られることを示している．しかし，この最終状態から隠れ部分群が**効率良く**（つまり $\mathrm{poly}(\log|G|)$ 回の演算で）同定できる POVM が存在するか否かはわかっていない．

**問題 5.6:（Fourier 変換による加法）** $|x\rangle \to |x + y \bmod 2^n\rangle$ を計算する量子回路を構築するタスクを考える．ここで $y$ は決まった定数，$0 \le x < 2^n$ である．これには $y = 1$ のような値に対して最初に量子 Fourier 変換を行い，次に単一 q ビット位相シフトを適用し，最後に Fourier 逆変換を行うのが 1 つの効率的方法であることを示せ．この方法でどんな $y$ の値が容易に加えられるか，また何回の演算が必要か？

### 5 章のまとめ： 量子 Fourier 変換とその応用

- $N = 2^n$ のとき量子 Fourier 変換：

$$|j\rangle = |j_1, \ldots, j_n\rangle \to \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i \frac{jk}{N}} |k\rangle \tag{5.81}$$

は次のように書けて，$\Theta(n^2)$ 個のゲートで実現できる．

$$\begin{aligned}|j\rangle \to \frac{1}{2^{n/2}} &\left(|0\rangle + e^{2\pi i 0.j_n}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0.j_{n-1}j_n}|1\rangle\right) \\ &\ldots \left(|0\rangle + e^{2\pi i 0.j_1 j_2 \ldots j_n}|1\rangle\right).\end{aligned} \tag{5.82}$$

- **位相推定：** $|u\rangle$ は固有値 $e^{2\pi i\varphi}$ を有するオペレータ $U$ の固有状態であるとする．初期状態 $|0\rangle^{\otimes t}|u\rangle$ から出発して，整数 $k$ に対して $U^{2^k}$ を実行できるとすると，（図 5.3 に示した）このアルゴリズムを使って状態 $|\tilde{\varphi}\rangle|u\rangle$ が効率的に得られる．ここで $\tilde{\varphi}$ は $\varphi$ を少なくとも $1 - \epsilon$ の確率

で，$t - \lceil \log(2 + \frac{1}{2\epsilon}) \rceil$ ビット精度で正確に近似する．

- **位数発見：** $N$ を法とする $x$ の位数は $x^r \bmod N = 1$ を満たす最小の整数 $r$ である．この数は $L$ ビットの整数 $x$ と $N$ に対する量子位相推定アルゴリズムを用いて $O(L^3)$ 回の演算で計算できる．
- **素因数分解：** $L$ ビットの整数 $N$ の素因数は，$N$ と互いに素なランダムな数 $x$ の位数を見出す問題に縮約することにより，演算階数 $O(L^3)$ で決定できる．
- **隠れ部分群問題：** 知られているすべての高速量子アルゴリズムは次の問題を解くことで記述できる：有限に生成された群 $G$ から有限の集合 $X$ への関数を $f$ とし，$f$ は部分群 $K$ の剰余類上で一定，かつ各剰余類で互いに異なるとする．$g \in G$，$h \in X$ に対してユニタリー変換 $U|g\rangle|h\rangle = |g\rangle|h \oplus f(g)\rangle$ を実行する量子ブラックボックスが与えられたとして，$K$ に対する生成集合を見出せ．

## 歴史と参考資料

Fourier 変換の定義は本章で考えた以上に一般化できる．一般的シナリオでは Fourier 変換は複素数 $\alpha_g$ の集合上で定義される．ここで指数 $g$ はある群 $G$ から選ばれる．本章では $G$ は $2^n$ を法とする整数の加法群であるとして $\mathbf{Z}_{2^n}$ で表した．Deutsch [Deu85] は群 $\mathbf{Z}_{2^n}$ 上の Fourier 変換は量子コンピュータ上に効率的に実現できることを示した — これは前の章で示した Hadamard 変換である．Shor [Sho94] はある特定の値 $m$ に対する群 $\mathbf{Z}_m$ 上の量子 Fourier 変換を量子コンピュータが効率良く実現できることを示して目覚ましい影響を及ぼした．この結果に刺激されて Coppersmith [Cop94]，Deutsch（未発表）および Cleve（未発表）が $\mathbf{Z}_{2^n}$ 上の量子 Fourier 変換を計算する簡単な量子回路を与え，本章ではこれを用いた．Cleve, Ekert, Macchiavello, Mosca [CEMM98]，および Griffiths と Niu [GN96] は独立に積公式 (5.4) を見出した．実際にはこの結果はもっと前に Danielson と Lanczos によって示されていた．式 (5.5) から始まる簡単化された証明は Zhou により示唆された．Griffiths, Niu [GN96] は問題 5.2 の量子 Fourier

変換測定の元になっている．

$\mathbf{Z}_{2^n}$ 上の Fourier 変換は Kitaev [Kit95] によって任意の有限な Abel 群上の Fourier 変換に一般化された．彼はまた問題 5.3 で示した形の位相推定手続きを導入した．Cleve, Ekert, Macchiavello, Mosca [CEMM98] も Shor と Kitaev の幾つかのテクニックを統合して 1 つの素晴らしい描像を示した．5.2 節はこれによっている．位相推定アルゴリズムは Mosca の博士論文 [Mos99] に詳しく記述されている．

Shor は量子位数発見アルゴリズムを 1994 年の影響力の強い論文 [Sho94] で発表し，離散対数と素因数分解問題は位数発見に縮約されることを指摘した．拡張された議論と参考文献を含む最終の論文は 1997 年に発表された [Sho97]．本書のアルゴリズムよりさらに高速化できる巧妙な乗算方法が，この論文で比較的素朴な乗算テクニックを使って議論されている．この高速乗算を用いると合成数 $n$ を素因数分解するに必要なリソースは本章の始めに述べたように $O(n^2 \log n \log\log n)$ となる．1995 年に Kitaev [Kit95] は一般の Abel 群の固定部分群を見出すアルゴリズムを発表し，これを使うと特別な場合として離散対数と素因数分解が解けることを示した．加えてこのアルゴリズムには Shor のアルゴリズムにはない幾つかの要素が含まれている．素因数分解に関する良い解説が Ekert，Jozsa [EJ96] により書かれている．DiVincenzo [DiV95a] も参考になる．連分数の議論は Hardy, Wright [HW60] の 10 章によっている．本書の執筆時点で最も効率の良い素因数分解の古典アルゴリズムは数体ふるい法である．これは A. K. Lenstra, H. W. Lenstra, Jr. が編集した論文集 [LL93] に述べられている．

量子アルゴリズムを拡張して隠れ部分群問題を解くことは多くの研究者が考えてきた．歴史的には Simon が最初に量子コンピュータは $f(x \oplus s) = f(x)$ を満たす隠れ周期を見つけられることを述べた [Sim94][Sim97]．実際 Shor は Simon の結果を一般化し，Simon の Hadamard 変換（$\mathbf{Z}_2^k$ 上の Fourier 変換）に代わって，$\mathbf{Z}_N$ を適用することによって彼の結果を得たのである．次いで Boneh と Lipton は隠れ部分群問題との関連に気付き，隠れ線形関数問題を解く量子アルゴリズムを発表した [BL95]．Jozsa は隠れ部分群問題に関連して，Deutsch-Jozsa, Simon, Shor それぞれのアルゴリズムを初めて一様に記述した [Joz97]．量子アルゴリズムの高速化における，Abel 群と非 Abel 群の高速 Fourier 変換アルゴリズムの役割を研究した Ekert と Jozsa の仕事 [EJ98] も洞察力に富むものであった．本

書 5.4 節の隠れ部分群問題の記述は Mosca と Ekert の枠組み [ME99][Mos99] に従っている．Cleve は置換の位数を見つける問題が，有界誤差の確率的な古典コンピュータに対して，指数関数的な数の演算を必要とすることを示した [Cle99]．この方法を Abel 群以外に一般化する試みは Ettinger，Høyer [EH99]，Roetteler, Beth [RB98]，Pueschel, Roetteler, Beth [PRB98]，Beals [BBC+98]，および Ettinger, Høyer, Knill [EHK99] により行われた．Beals は対称群上の量子 Fourier 変換の構築についても述べている．これまでにこれらの結果によって，$O(\log|G|)$ 回のオラクル呼び出しで非 Abel 群に対する隠れ部分群問題を解く量子アルゴリズムが**存在する**ことがわかっている．しかし，これが多項式時間で実現できるかどうかはわかっていない（問題 5.5）．

# 第6章　量子探索アルゴリズム

多くの都市が載っている地図があるとして，地図上の全都市を巡る最短ルートを決めたいとする．このルートを見つける簡単なアルゴリズムは，都市を通る可能なルートをすべて探して，どのルートが最短になるか走行記録を作ることである．$N$ 個の可能なルートがあるとき，この方法により古典コンピュータ上で最短ルートを決めるには，明らかに $O(N)$ 回の演算を必要とする．注目すべきは**量子探索アルゴリズム** (quantum search algorithm) あるいは **Grover のアルゴリズム**(Grover's algorithm) と呼ぶアルゴリズムである．これによれば探索が実質的に高速化されて $O(\sqrt{N})$ 回の演算で済む．さらに，ここで述べるルート発見の例以外にも，(すべてではないが) 多くの発見的探索手法を使う古典アルゴリズムを高速化できるという意味で，量子探索アルゴリズムは**一般的**な方法である．

本章では高速量子探索アルゴリズムについて説明する．この基本的アルゴリズムを 6.1 節で述べる．6.2 節では 4.7 節に示した量子シミュレーションアルゴリズムに基づいて，別の観点からこのアルゴリズムを導く．次に，このアルゴリズムの 3 つの重要な応用について述べる．6.3 節は量子計数，6.4 節で **NP** 完全問題の解の高速化，6.5 節は構造を持たないデータベースの探索である．平方根以上の高速化を実現する良い探索アルゴリズムの改善を望むかも知れないが，これは可能でないことを 6.6 節で示す．結論としてこの高速化限界は，たいていの構造を持たない問題に成立することを 6.7 節に示す．

# 6.1　量子探索アルゴリズム

最初に 3.1.1 項（第 I 巻）で見たのと同様に，**オラクル** (oracle) を使って探索アルゴリズムの舞台を作る．これによって探索手続きを非常に一般的に記述できて，その働きを可視化して性能を確かめる幾何学的方法を示すことができる．

## 6.1.1　オラクル

$N$ 個の要素を持つ探索空間を探索するとする．各要素を直接探索する代わりに 0 から $N-1$ の範囲の数であるこの要素の**指数** (index) に着目する．便宜上 $N=2^n$ と仮定して指数は $n$ ビットで蓄積でき，探索問題は正確に $M$ 個の解を持つとする．ここで $1 \leq M \leq N$ である．探索問題の特定の事例を便宜上関数 $f$ で表し，$f$ の入力は 0 から $N-1$ の範囲の整数 $x$ であるとする．定義として $x$ が探索問題の解ならば $f(x)=1$，解でなければ $f(x)=0$ とする．

仮に探索問題の解を**認識**する能力を持つ**量子オラクル** (quantum oracle) — 内部の働きは後で議論するがこの段階では重要でないブラックボックス— が提供されているとする．オラクルの認識結果は**オラクル q ビット**を利用して信号に変わる．正確に言えばオラクルはユニタリーオペレータ $O$ であり，計算基底に対する次の作用で定義される：

$$|x\rangle|q\rangle \xrightarrow{O} |x\rangle|q \oplus f(x)\rangle, \tag{6.1}$$

ここで $|x\rangle$ は指数レジスタ，$\oplus$ は 2 を法とする和，オラクル q ビット $|q\rangle$ はもし $f(x)=1$ ならば反転し，そうでなければそのままの値をとる単一 q ビットである．$x$ が探索問題の解かどうかをチェックするには $|x\rangle|0\rangle$ を用意し，オラクルを作用させ，オラクル q ビットが $|1\rangle$ に反転するかどうかを見ればわかる．

1.4.4 項（第 I 巻）の Deutsch-Jazsa のアルゴリズムにおいて行ったように，量子探索アルゴリズムでは初期状態 $(|0\rangle-|1\rangle)/\sqrt{2}$ にあるオラクル q ビットにオラクルを適用するのが便利である．もし $x$ が探索問題の解でなければオラクルを $|x\rangle(|0\rangle-|1\rangle)/\sqrt{2}$ に適用しても状態は変化しない．それに対して $x$ が探索問題の解ならばオラクルの作用で $|0\rangle$ と $|1\rangle$ が入れ替わり，最終状態が $-|x\rangle(|0\rangle-|1\rangle)/\sqrt{2}$

となる．したがって，オラクルの動作は：

$$|x\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) \stackrel{O}{\rightarrow} (-1)^{f(x)}|x\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right). \tag{6.2}$$

オラクル q ビットの状態は変化しないことに注意する．量子探索アルゴリズムを通じてこの状態 $(|0\rangle-|1\rangle)/\sqrt{2}$ は変化しないので，アルゴリズムのこれ以降の議論では省略して記述を簡単にする．

この便法を用いるとオラクルの働きは次のように書ける：

$$|x\rangle \stackrel{O}{\rightarrow} (-1)^{f(x)}|x\rangle. \tag{6.3}$$

オラクルが解の位相をシフトさせることを，探索問題の解に**マーク**を付けるという．$N$ 個の項目を探索して $M$ 個の解を持つ問題に対して量子コンピュータ上で解を得るには，探索オラクルを $O(\sqrt{N/M})$ 回適用するだけでよいことがわかる．

実際にどう働くかを示さずにオラクルを議論するのは，少し抽象的であり紛らわしくもある．まるでオラクルが探索問題の答をあらかじめ**知っている**かのようである．このようなオラクルを参照する量子探索アルゴリズムの用途は何であろうか?! その答は探索問題の解を**知っている** (know) ことと，解であることを**認識する** (recognize) ことの違いであり，必ずしも前者ができなくても後者を行うことは可能である点が重要である．

これを示す簡単な例は素因数分解の問題である．大きな数 $m$ が与えられそれが 2 つの素数 $p$ と $q$ の積であると教えられているとする — 同様の状況が RSA 公開鍵暗号を破ろうとするときに起きる (付録 E)．古典コンピュータ上で $p$ と $q$ を決めるための明らかな方法は 2 から $m^{1/2}$ までのすべての数を対象に 2 つの素数の小さいほうを**探索**することである．つまり小さいほうの素数が求まるまで $m$ を 2 から $m^{1/2}$ の間の数で割り算を順次試行する．他の素数は $m$ を小さいほうの素数で割れば得られる．明らかにこの探索ベースの方法には古典コンピュータ上ではほぼ $m^{1/2}$ 回の割り算が要求される．

量子探索アルゴリズムはこのプロセスを高速化するのに使える．定義により状態 $|x\rangle$ の入力に対するオラクルの作用は，$m$ を $x$ で割って割り切れるかどうかを確かめ，もし割り切れればオラクル q ビットを反転する．このオラクルを用いた量子探索アルゴリズムを適用すると，高い確率で 2 つの素数のうちで小さいほうが

作れる．しかしこのアルゴリズムが動くには，オラクルを実行する効率的回路を構築する必要がある．これを行う方法は可逆計算テクニックの演習である．はじめに，もし $x$ が $m$ を整除するならば関数 $f(x)=1$，そうでなければ $f(x)=0$ と定義する．割り算が成功するかどうかを $f(x)$ が教えてくれるわけである．3.2.5項（第I巻）で議論した可逆計算のテクニックを使って，割り算の試行を行うための通常の（非可逆な）古典回路を変形して，$(x,q)$ を取り入れて $(x,q\oplus f(x))$ に変換する古典的な可逆回路を構成する．ここで入力 $(x,q)$ は最初 $x$ に設定した入力レジスタと最初 $q$ に設定した1ビット出力レジスタを表す．この可逆回路のリソースコストは係数2の範囲で割り算の試行を行う古典的非可逆回路と同じであり，したがって両方の回路は本質的に同じリソースを消費すると見なす．さらに古典可逆回路はオラクルに要求されるような $|x\rangle|q\rangle$ を $|a\rangle|q\oplus f(x)\rangle$ に変える量子回路に直ちに変換できる．重要な点は $m$ **の素因数を知らなくても，それを見て探索問題の解が認識できるオラクルを明示的に構築できる**ことである．このオラクルと量子探索アルゴリズムを用いると，オラクルを $O(m^{1/4})$ 回参照することによって2から $m^{1/2}$ の範囲の探索ができる．つまり古典アルゴリズムの $m^{1/2}$ 回に代わって，割り算をおよそ $m^{1/4}$ 回試行するだけでよい！

この素因数分解の例は概念的な興味はあるが実際的ではない．すべての可能な除数を探索するより，もっと高速で働く古典的な探索アルゴリズムが存在するからである．しかし，この例は量子探索アルゴリズムを応用する一般的方法を示しており，探索ベースのテクニックに依存する古典アルゴリズムが，量子探索アルゴリズムを使って高速化できる．本章ではこの後量子探索アルゴリズムが **NP** 完全問題の解の高速化に本当に役立つシナリオを調べる．

### 6.1.2　手続き

探索アルゴリズムを模式的に描くと図6.1のような動作をする．アルゴリズム自体は単一の $n$ - q ビットレジスタを使用する．オラクル内部の作業は付加的な作業 q ビットを必要とすることも含めて，量子探索アルゴリズム自体の記述には重要でない．アルゴリズムのゴールはオラクルの適用回数を可能な限り最少にして，探索問題の解を見つけることである．

アルゴリズムはコンピュータの状態 $|0\rangle^{\otimes n}$ から始まる．Hadamard 変換を用い

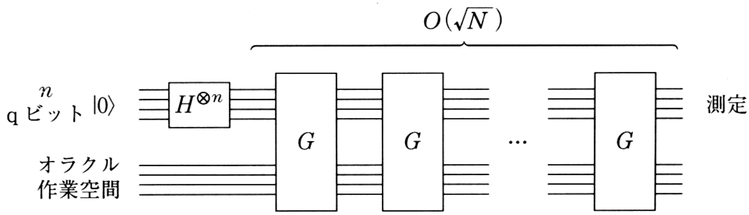



**図 6.1:** 量子探索アルゴリズムの模式的回路図．オラクル実行には作業 q ビットが必要になるが，量子探索アルゴリズム解析には $n$ 個の q ビットレジスタだけを考える．

て等しい重ね合せ状態にする：

$$|\psi\rangle = \frac{1}{N^{1/2}} \sum_{x=0}^{N-1} |x\rangle. \tag{6.4}$$

次に **Grover の反復** (Grover iteration) あるいは **Grover のオペレータ** (Grover operator) と呼ぶ量子サブルーチン $G$ を繰り返し適用して量子探索アルゴリズムを構成する．Grover の反復は図 6.2 に示すように，4 つのステップに分けられる：

(1) オラクル $O$ を適用する．

(2) Hadamard 変換 $H^{\otimes n}$ を適用する．

(3) コンピュータに条件付き位相シフトを実行し，$|0\rangle$ 以外のすべての計算基底状態に $-1$ の位相シフトを与える．

$$|x\rangle \rightarrow -(-1)^{\delta_{x0}}|x\rangle. \tag{6.5}$$

(4) Hadamard 変換 $H^{\otimes n}$ を適用する．

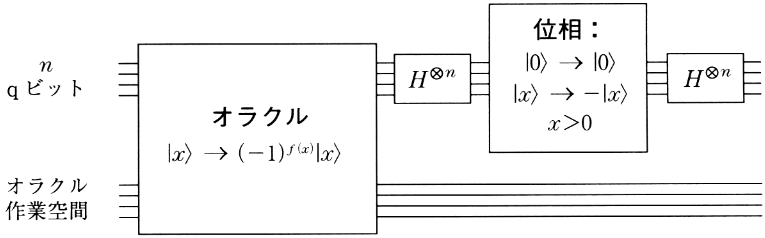



**図 6.2:** Grover の反復 $G$ の回路．

**演習 6.1:** Grover の反復における位相シフトに対応するユニタリーオペレータは $2|0\rangle\langle 0| - I$ であることを示せ．

Grover の反復における各演算は量子コンピュータ上で効率的に実行できる．ステップ (2) と (4) における Hadamard 変換は各々 $n = \log(N)$ 回の演算を必要とする．ステップ 3 の条件付き位相シフトは 4.3 節のテクニックを用いて $O(n)$ 個のゲートで実行できる．オラクル呼び出しのコストは応用の種類に依存する．取り敢えず Grover の反復を 1 回のオラクル呼び出しで行うとする．ステップ (2), (3), (4) を組み合わせた効果は：

$$H^{\otimes n}(2|0\rangle\langle 0| - I)H^{\otimes n} = 2|\psi\rangle\langle\psi| - I, \tag{6.6}$$

ここで $|\psi\rangle$ は等加重の重ね合せ状態 (6.4) である．したがって，Grover の反復 $G$ は $G = (2|\psi\rangle\langle\psi| - I)O$ と書ける．

**演習 6.2:** 演算 $(2|\psi\rangle\langle\psi| - I)$ を一般の状態 $\sum_k \alpha_k|k\rangle$ に適用すると

$$\sum_k \left[-\alpha_k + 2\langle\alpha\rangle\right]|k\rangle \tag{6.7}$$

となることを示せ．ここで $\langle\alpha\rangle \equiv \sum_k \alpha_k/N$ は $\alpha_k$ の平均値である．この理由で $(2|\psi\rangle\langle\psi| - I)$ は**平均値に関する反転** (inversion) 演算と呼ばれる．

### 6.1.3　幾何学的可視化

Grover の反復は何をするのか？ $G = (2|\psi\rangle\langle\psi| - I)O$ であることを述べた．実際に Grover の反復は，初期ベクトル $|\psi\rangle$ と探索問題の解の一様な重ね合せからなる状態が張る，2 次元空間中の**回転** (rotation) と見なせることを示そう．これを見るには $\sum_x'$ が探索問題の解である全 $x$ に関する総和を表し，$\sum_x''$ は探索問題の解でない全 $x$ に関する総和を表す便法を用いると便利である．正規化された次の状態を定義する：

$$|\alpha\rangle \equiv \frac{1}{\sqrt{N-M}}\sum_x{}'' |x\rangle, \tag{6.8}$$

$$|\beta\rangle \equiv \frac{1}{\sqrt{M}}\sum_x{}' |x\rangle. \tag{6.9}$$

簡単な代数計算で初期状態 $|\psi\rangle$ を書き換えると：

$$|\psi\rangle = \sqrt{\frac{N-M}{N}}|\alpha\rangle + \sqrt{\frac{M}{N}}|\beta\rangle. \tag{6.10}$$

したがって，量子コンピュータの初期状態は $|\alpha\rangle$ と $|\beta\rangle$ が張る空間にある．

$|\alpha\rangle$ と $|\beta\rangle$ で定義される平面においてオラクル演算はベクトル $|\alpha\rangle$ に関する**反射** (reflection) に相当することがわかると，$G$ の効果が簡潔に理解できる．つまり $O(a|\alpha\rangle + b|\beta\rangle) = a|\alpha\rangle - b|\beta\rangle$ である．同様に $2|\psi\rangle\langle\psi| - I$ は $|\alpha\rangle$ と $|\beta\rangle$ で定義される平面でベクトル $|\psi\rangle$ に関する反射を行う．そして 2 つの反射の積は回転である！ これより状態 $G^k|\psi\rangle$ はすべての $k$ に対して $|\alpha\rangle$ と $|\beta\rangle$ が張る空間に留まる．これから回転角もわかる．$\cos\theta/2 = \sqrt{(N-M)/N}$ とすると $|\psi\rangle = \cos\theta/2\ |\alpha\rangle + \sin\theta/2\ |\beta\rangle$．図 6.3 が示すように $G$ を構成する 2 つの反射によって $|\psi\rangle$ は次のように変換される．

$$G|\psi\rangle = \cos\frac{3\theta}{2}|\alpha\rangle + \sin\frac{3\theta}{2}|\beta\rangle. \tag{6.11}$$

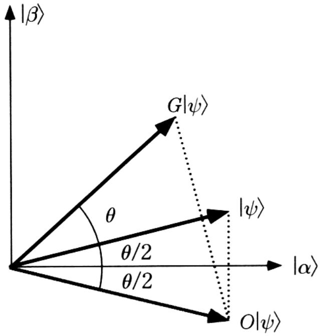



**図 6.3:** 単一の Grover の反復 $G$ の働き：状態ベクトルは探索問題のすべての解の重ね合せ $|\beta\rangle$ の方向に $\theta$ だけ回転する．最初に状態は $|\beta\rangle$ と直交する状態 $|\alpha\rangle$ から角度 $\theta/2$ だけ傾いている．オラクル演算 $O$ によってその状態は状態 $|\alpha\rangle$ に関して反射され，次に演算 $2|\psi\rangle\langle\psi| - I$ によって $|\psi\rangle$ に関して反射される．図では混乱を避けるために $|\alpha\rangle$ と $|\beta\rangle$ を少し長めにしてある（すべての状態は単位ベクトルでなければならない）．Grover の反復を繰り返すと状態ベクトルは $|\beta\rangle$ に近づき，その点で計算基底で観測すると高い確率で探索問題の解が出力される．このアルゴリズムの効率が顕著なのは $\theta$ が $\Omega(\sqrt{M/N})$ で振る舞うので，状態ベクトルを $|\beta\rangle$ 近くまで回転するには $G$ を $O(\sqrt{N/M})$ 回適用するだけで済むからである．

したがって回転角は事実上 $\theta$ である．$G$ を連続して適用すると状態は次のように変換される：

$$G^k|\psi\rangle = \cos\left(\frac{2k+1}{2}\theta\right)|\alpha\rangle + \sin\left(\frac{2k+1}{2}\theta\right)|\beta\rangle. \tag{6.12}$$

まとめると，$G$ は $|\alpha\rangle$ と $|\beta\rangle$ が張る 2 次元空間における回転であり，1 回の適用によって状態を $\theta$ ラジアンだけ回転する．Grover の反復を繰り返すと状態ベクトルを $|\beta\rangle$ に近づける．これが生じると計算基底で観測することで $|\beta\rangle$ 中に重ね合わされていた出力，つまり探索問題の解の 1 つが高い確率で現れる！ $N=4$ の探索問題の例をコラム 6.1 に示す．

**演習 6.3:** 基底 $|\alpha\rangle$, $|\beta\rangle$ において Grover の反復は次のように書けることを示せ：

$$G = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}, \tag{6.13}$$

ここで $\theta$ は次式のように選んだ 0 から $\pi/2$ の間の実数である（簡単のために $M \le N/2$ と仮定するがこの制限は間もなく取り除く）：

$$\sin\theta = \frac{2\sqrt{M(N-M)}}{N}. \tag{6.14}$$

### 6.1.4　性　能

$|\psi\rangle$ を $|\beta\rangle$ 近くまで回転するには Grover の反復を何回繰り返さねばならないか？ システムの初期状態は $|\psi\rangle = \sqrt{(N-M)/N}|\alpha\rangle + \sqrt{M/N}|\beta\rangle$ であり，$\arccos\sqrt{M/N}$ ラジアンだけ回転するとシステムを $|\beta\rangle$ に一致できる．$\mathrm{CI}(x)$ は実数 $x$ に最も近い整数 — 例えば $\mathrm{CI}(3.5)=3$ のように慣習で 0.5 は切り捨てる — であるとする．Grover の反復の繰り返し数を

$$R = \mathrm{CI}\left(\frac{\arccos\sqrt{M/N}}{\theta}\right) \tag{6.15}$$

とすると $|\psi\rangle$ は $|\beta\rangle$ から角度 $\theta/2 \le \pi/4$ の範囲まで回転する．計算基底で状態を観測すると少なくとも確率 1/2 で探索問題の解が得られる．例えば $M \ll N$ の

とき $\theta \approx \sin\theta \approx 2\sqrt{M/N}$ であり，したがって最終状態の角度誤差はたかだか $\theta/2 \approx \sqrt{M/N}$，誤差はたかだか $M/N$ である．$R$ は解の数 $M$ に依存するが解自体の性質に依存せず，したがって $M$ がわかっていればここに述べたように量子探索が適用できることに注意する．6.3 節で探索アルゴリズムを適用する際の $M$ に関する知識の必要性も取り去る方法を説明する．

式 (6.15) の形は量子探索アルゴリズムを実行するときの，オラクル呼び出しの回数を正確に決める式として便利である．しかし $R$ の本質的振る舞いを要約した簡単な式があればもっと便利であろう．これを実現するために式 (6.15) より $R \le \lceil \pi/2\theta \rceil$ に留意すると $\theta$ の下界が $R$ の上界を与える．取り敢えず $M \le N/2$ と仮定すると

$$\frac{\theta}{2} \ge \sin\frac{\theta}{2} = \sqrt{\frac{M}{N}}, \tag{6.16}$$

これから要求される反復数の簡潔な上界として次式を得る：

$$R \le \left\lceil \frac{\pi}{4}\sqrt{\frac{N}{M}} \right\rceil. \tag{6.17}$$

つまり高い確率で探索問題の解を得るには，Grover の反復を（したがってオラクル呼び出しも）$R = O(\sqrt{\frac{N}{M}})$ 回実行しなければならない．これは古典的に要求されるオラクル呼び出し回数 $O(N/M)$ に比べて 2 乗の改善になる．$M = 1$ の場合に対する量子探索アルゴリズムを以下にまとめる．

**アルゴリズム：量子探索**

**入力：** (1) 変換 $O|x\rangle|q\rangle = |x\rangle|q \oplus f(x)\rangle$ を実行するオラクルのブラックボックス．ここで $x_0$ に対して $f(x_0) = 1$，それ以外のすべての $0 \le x \le 2^n$ に対して $f(x) = 0$.

(2) 状態 $|0\rangle$ にある $n$ 個の q ビット．

**出力：** $x_0$.

**演算回数：** $O(\sqrt{2^n})$ 回の演算．成功確率 $O(1)$

**手続き：**

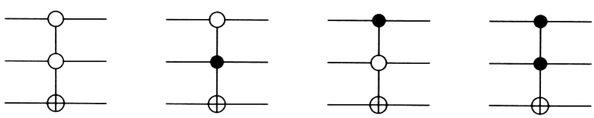
1. $|0\rangle^{\otimes n}|0\rangle$　　初期状態
2. $\rightarrow \dfrac{1}{\sqrt{2^n}}\displaystyle\sum_{x=0}^{2^n-1}|x\rangle\left[\dfrac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$　　最初の $n$ - q ビットに $H^{\otimes n}$，最後の q ビットに $HX$ を適用
3. $\rightarrow [(2|\psi\rangle\langle\psi|-I)O]^R\dfrac{1}{\sqrt{2^n}}\displaystyle\sum_{x=0}^{2^n-1}|x\rangle\left[\dfrac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$

   $\approx |x_0\rangle\left[\dfrac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$　　Grover 反復を $R\approx\lceil\pi\sqrt{2^n}/4\rceil$ 回適用
4. $\rightarrow x_0$　　最初の $n$ 個の q ビットを測定

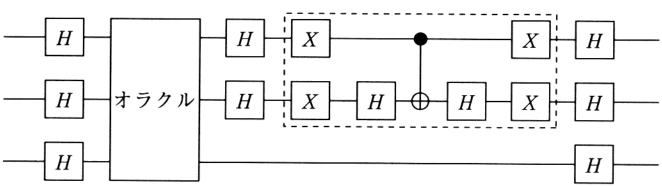
**演習 6.4:** 上と同様であるが，多数の解（$1<M<N/2$）がある場合の量子探索アルゴリズムのステップを明示的に書け．

### コラム 6.1: 量子探索：2 ビットの例

サイズ $N=4$ の探索空間において，量子探索アルゴリズムがどのように働くかの例を示す．$f(x_0)=1$ なる $x_0$ を除くすべての $x$ に対して，$f(x)=0$ となるオラクルは次の 4 回路のうちの 1 つをとる．



この図で左から右にかけて $x_0=0$, 1, 2, 3 に対応し，上の 2 つの q ビットは質問 $x$ を，下の q ビットはオラクルの応答を表す．最初の Hadamard 変換と 1 回の Grover 反復 $G$ を実行する量子回路は：




最初上の 2 つの q ビットは $|0\rangle$ に，下の q ビットは $|1\rangle$ に初期化されている．点線枠で囲んだゲートは条件付き位相シフト演算 $2|00\rangle\langle 00|-I$ を実行する．$x_0$

を得るのに $G$ を何回繰り返さねばならないか？ 式 (6.15) で $M=1$ とすると要求される繰り返しは 1 回以下であることがわかる．式 (6.14) で $\theta=\pi/3$ なのでこの特定の場合，完全に $x_0$ を得るに要する繰り返し回数は**正確に 1 回**だけでよい．図 6.3 の幾何学的図で初期状態 $|\psi\rangle=(|00\rangle+|01\rangle+|10\rangle+|11\rangle)/2$ は $|\alpha\rangle$ から $30°$ であり，$\theta=60°$ の回転 1 回で $|\psi\rangle$ は $|\beta\rangle$ に移る．オラクルを 1 回使うだけで上の 2 つの q ビットを測定すると $x_0$ が得られることを，量子回路で確かめることができる．これに対して古典コンピュータ — あるいは古典回路 — では 4 つのオラクルの差を見つけるために平均で 2.25 回の質問をしなければならない！

探索問題の解が要素の半分以上，つまり $M>N/2$ の場合はどうなるか？ $M$ が $N/2$ から $N$ に変化するに従い式 $\theta=\arcsin(2\sqrt{M(N-M)}/N)$（式 (6.14) 参照）により角度 $\theta$ は減少する．その結果，$M>N/2$ に対して探索アルゴリズムに必要な反復回数は $M$ と共に**増加する**．直観的にこれは探索問題の性質としてばかげているように見える．解の数が増えるに従って問題の解を見つけるのは容易になるはずである．この問題を巡って少なくとも 2 つの途がある．もしあらかじめ $M$ が $N/2$ 以上であることがわかっているならば，探索空間からランダムに要素を取り上げてオラクルを使って解であるかどうかを検査する．このアプローチの成功確率は少なくとも 1/2 でありオラクルの呼び出しは 1 回のみである．不利な点はあらかじめ解 $M$ の数がわからないことである．

$M\geq N/2$ であるかどうかわからない場合，別のアプローチが使える．このアプローチはそれ自体興味あるものであり，6.3 節で述べる探索問題の解の数を数える量子アルゴリズムが簡単に解析できるという便利な応用がある．その考え方はいずれも解でない $N$ 個の付加的な項目を加えて探索空間の要素数を倍にするものである．この結果新しい探索空間の半分以下の項目が解ということになる．これは単一 q ビット $|q\rangle$ を探索指数に追加して探索すべき項目数を倍の $2N$ にする．項目が探索問題の解であってしかも余分のビットが 0 になる項目のみを選び出すように，新しく**拡大した**オラクル $O'$ を構成する．演習 6.5 において $O$ を 1 回呼び出すことによりオラクル $O'$ を構築する方法を説明してもらう．新しい探索問題は $2N$ 個の要素のうちで解は $M$ 個だけなので，新しいオラクル $O'$ で探索アルゴリ

ズムを走らせると要求されるオラクル $O'$ 呼び出しはたかだか $R = \pi/4\sqrt{2N/M}$ であり，$O(\sqrt{N/M})$ 回の $O$ 呼び出しが探索の実行に必要となる．

**演習 6.5:** 拡大したオラクル $O'$ は余分の q ビット $|q\rangle$ を用い，$O$ を 1 回と基本的量子ゲートを適用することで構成できることを示せ．

量子探索アルゴリズムは広範囲に利用できて，その幾つかを以後の節で調べる．このアルゴリズムの利便性が高い理由は，探索を行う問題に対して如何なる特定の構造も仮定しないことにある．これは「ブラックボックス」オラクルの形で問題を提起する大きな利点であり，以後本章では必要に応じてこの観点を踏襲する．もちろん具体的応用にオラクルをどう実行するか理解する必要があるので，個別の具体的問題を扱うときにはオラクルの実現法について明示的に述べる．

**演習 6.6:** コラム 6.1 の 2 番目の図にある点線の箱にあるゲートが，重要でないグローバル位相を除いて，条件付き位相シフト演算 $2|00\rangle\langle 00| - I$ を実行することを証明せよ．

## 6.2　量子シミュレーションとしての量子探索

量子探索アルゴリズムが正しいことは容易に証明できるが，何も知らない状態からどうすればそのようなアルゴリズムを考え出せるかは決して明らかでない．本節では量子アルゴリズム設計というトリッキーなタスクに関して直観を与えることを目指して，量子探索アルゴリズムを「導く」発見的方法の概略を述べる．有益な副産物として，**決定性**の量子探索アルゴリズムが得られる．我々のゴールは一般性ではなく洞察力を得ることなので，簡単のために探索問題は 1 つの解 — これを $x$ と表示する — しか持たないと仮定する．

我々の方法は 2 段階からなる．最初に探索問題を解く **Hamiltonian** を推定する．正確に言えば解 $x$ と初期状態 $|\psi\rangle$ に依存し，量子システムが Hamiltonian $H$ に従ってあるあらかじめ決められた時間後に $|\psi\rangle$ から $|x\rangle$ に変化するような $H$ を書き下す．一度そのような Hamiltonian と初期状態が見つかれば第 2 段階に進み，量子回路を使って Hamiltonian 動作のシミュレーションを試行する．驚くべきことに，この手続きに従うと直ぐに量子探索アルゴリズムが導ける！ 我々はす

でに問題 4.3 において，量子回路の普遍性を調べるためにこの 2 段階手続きに出会っており，これが量子探索の研究にも役立つ．

アルゴリズムは状態 $|\psi\rangle$ にある量子コンピュータからスタートするとする．後になってから $|\psi\rangle$ に制約を課すが，アルゴリズムの振る舞いを理解するまでは $|\psi\rangle$ について何も決めないでおくのが便利である．量子探索のゴールは $|\psi\rangle$ を $|x\rangle$ に変化させるか，あるいは何かその近似を行うことである．うまくそのような時間発展をさせる Hamiltonian はどのようにして推定すればいいか？ 簡単なものが良いという考えに立てば，$|\psi\rangle$ と $|x\rangle$ の項のみから Hamiltonian が構成されると推定すべきであろう．したがって，Hamiltonian は $|\psi\rangle\langle\psi|$, $|x\rangle\langle x|$, $|\psi\rangle\langle x|$ および $|x\rangle\langle\psi|$ のような項の和であるに違いない．この線に沿った最も簡単な選択は：

$$H = |x\rangle\langle x| + |\psi\rangle\langle\psi| \tag{6.18}$$

$$H = |x\rangle\langle\psi| + |\psi\rangle\langle x|. \tag{6.19}$$

これら両方の Hamiltonian から量子探索アルゴリズムが導かれることがわかる！しかし当面式 (6.18) の Hamiltonian の解析に集中する．2.2.2 項（第 I 巻）より初期状態 $|\psi\rangle$ にあって Hamiltonian $H$ に従い時間発展する量子システムは時間 $t$ の後で：

$$\exp(-iHt)|\psi\rangle. \tag{6.20}$$

直観的にはなかなか良さそうに見える：小さな $t$ に対して時間発展は $|\psi\rangle$ を $(I - itH)|\psi\rangle = (1-it)|\psi\rangle - it\langle x|\psi\rangle|x\rangle$ に変える効果を持つ．つまり $|\psi\rangle$ ベクトルは僅かに $|x\rangle$ 方向に回転される．$\exp(-iHt)|\psi\rangle = |x\rangle$ となるような $t$ が存在するかどうかを決めることをゴールとして，実際に完全な解析をしてみよう．明らかに $|x\rangle$ と $|\psi\rangle$ が張る 2 次元空間に話を限ってよい．Gram-Schmidt の手続きに従って $|x\rangle$ と $|y\rangle$ がこの空間の直交基底を構成するように $|y\rangle$ を選び，$\alpha^2+\beta^2=1$ なるある $\alpha$ と $\beta$ に対して $|\psi\rangle = \alpha|x\rangle + \beta|y\rangle$ とする．便宜上 $|x\rangle$ と $|y\rangle$ の位相は $\alpha$ と $\beta$ が負でない実数であるように選ぶ．$|x\rangle, |y\rangle$ の基底において

$$\begin{aligned} H &= \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} \alpha^2 & \alpha\beta \\ \alpha\beta & \beta^2 \end{bmatrix} = \begin{bmatrix} 1+\alpha^2 & \alpha\beta \\ \alpha\beta & 1-\alpha^2 \end{bmatrix} \\ &= I + \alpha(\beta X + \alpha Z). \end{aligned} \tag{6.21}$$

したがって

$$\exp(-iHt)|\psi\rangle = \exp(-it)\Big[\cos(\alpha t)|\psi\rangle - i\sin(\alpha t)(\beta X + \alpha Z)|\psi\rangle\Big]. \quad (6.22)$$

グローバル位相因子 $\exp(-it)$ を無視して，簡単な代数計算で $(\beta X+\alpha Z)|\psi\rangle = |x\rangle$ が示せる．時間 $t$ 後のシステムの状態は：

$$\cos(\alpha t)|\psi\rangle - i\sin(\alpha t)|x\rangle. \quad (6.23)$$

したがって時刻 $t = \pi/2\alpha$ でシステムを観測すると，確率 **1** で結果 $|x\rangle$ が得られ，探索問題の解が見つかる！ 不幸なことに観測時間が $|\psi\rangle$ の $|x\rangle$ 成分である $\alpha$ に依存し，したがって決定しようとしている $x$ に依存する．これを解決する明らかな方法はすべての $|x\rangle$ に対して同じ $\alpha$ を選ぶこと，つまり $|\psi\rangle$ を次の一様な重ね合せに選ぶことである：

$$|\psi\rangle = \frac{\sum_x |x\rangle}{\sqrt{N}}. \quad (6.24)$$

このように選ぶとすべての $x$ に対して $\alpha = 1/\sqrt{N}$ となり，観測時間 $t = \pi\sqrt{N}/2$ は $x$ の値を知る必要がなくなる．状態 (6.24) は Hadamard 変換によって作れることがわかっているという明らかな利点もある．

Hamiltonian (6.18) はベクトル $|\psi\rangle$ を $|x\rangle$ に回転することがわかった．Hamiltonian (6.18) をシミュレートする量子回路を見出して量子探索アルゴリズムを得ることができるだろうか？ 4.7 節の方法を適用すると $H$ をシミュレートする自然な方法は，短い時間増分 $\Delta t$ の間に Hamiltonian $H_1 \equiv |x\rangle\langle x|$ と $H_2 \equiv |\psi\rangle\langle\psi|$ を交互にシミュレートすることである．これらの Hamiltonian は 4 章の方法を用いて容易にシミュレートできて図 6.4，図 6.5 に示すようになる．

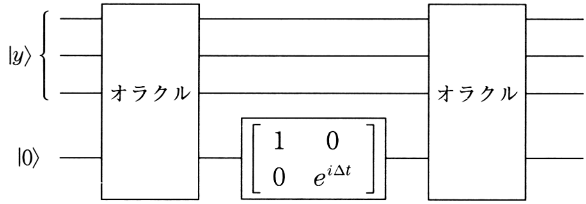



**図 6.4:** 2 回のオラクル呼び出しを使って演算 $\exp(-i|x\rangle\langle x|\Delta t)$ を実現する回路．

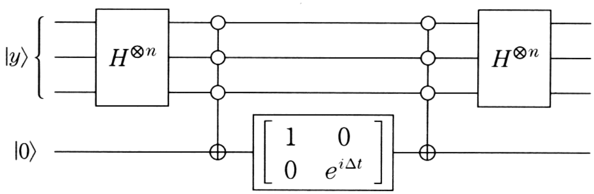



**図 6.5:** 式 (6.24) の $|\psi\rangle$ に対して演算 $\exp(-i|\psi\rangle\langle\psi|\Delta t)$ を実現する回路.

**演習 6.7:** 図6.4と6.5に示した回路が演算 $\exp(-i|x\rangle\langle x|\Delta t)$ と $\exp(-i|\psi\rangle\langle\psi|\Delta t)$ をそれぞれ実行することを証明せよ．ここで $|\psi\rangle$ は式 (6.24) で与えられる．

量子シミュレーションに要求されるオラクルの呼び出し回数は，合理的に正確な結果を得るのにどれ位時間ステップを小さくする必要があるかで決まる．精度 $O(\Delta t^2)$ を与える長さ $\Delta t$ のシミュレーションステップを用いるとする．必要とする全ステップ数は $t/\Delta t = \Theta(\sqrt{N}/\Delta t)$ であり，したがって累積誤差は $O(\Delta t^2 \times \sqrt{N}/\Delta t) = O(\Delta t\sqrt{N})$ となる．合理的に高い成功確率を得るには誤差が $O(1)$ である必要があり，$\Delta t = \Theta(1/\sqrt{N})$，したがってオラクル呼び出し回数が $O(N)$ となることを意味している — これは古典的解より良くはない！ もっと正確な — 例えば $O(\Delta t^3)$ 精度の — 量子シミュレーション法を用いるとどうなるか？ この場合の累積誤差は $O(\Delta t^2\sqrt{N})$ であり，合理的な成功確率を達成するには $\Delta t = \Theta(N^{-1/4})$，オラクル呼び出しの全回数は $O(N^{3/4})$ となる．これは紛れもなく古典的場合より改善されているが，まだ6.1節の量子探索アルゴリズムの性能ほど良くはない！ 一般により正確な量子シミュレーションテクニックを使えば，シミュレーションに必要なオラクルの呼び出し回数が減らせる．

**演習 6.8:** 精度 $O(\Delta t^r)$ でシミュレーションステップを実行するとする．合理的精度で $H$ をシミュレートするに必要なオラクルの呼び出し回数は，$O(N^{r/2(r-1)})$ であることを示せ．$r$ が大きくなるに従って $N$ の指数が $1/2$ に近づくことに注意する．

これまで4.7節の量子シミュレーションの一般的結果を用いて，Hamiltonian $H$ の量子シミュレーションにおける精度を解析してきた．もちろんこの事例では一般の場合でなく特定の Hamiltonian を取り扱っており，一般的解析によるよりも時間 $\Delta t$ のシミュレーションステップの効果を明示的に計算できると興味深

い．どんな特定のシミュレーション法に対してもこれを行うことができる — シミュレーションステップの効果を調べるのは少し退屈であるが，本質的に簡単な計算である．出発点は明らかに最低次のシミュレーションテクニックの効果 — つまり $\exp(-i|x\rangle\langle x|\Delta t)\exp(-i|\psi\rangle\langle\psi|\Delta t)$ または $\exp(-i|\psi\rangle\langle|\psi|\Delta t)\exp(-i|x\rangle\langle x|\Delta t)$ の一方または両方 — を明示的に計算することである．2つの結果は本質的に同じなので，

$$U(\Delta t) \equiv \exp(-i|\psi\rangle\langle|\psi|\Delta t)\exp(-i|x\rangle\langle x|\Delta t)$$

に焦点を絞る．明らかに $U(\Delta t)$ は $|x\rangle\langle x|$ と $|\psi\rangle\langle\psi|$ が張る空間のみに有意に作用するので，基底 $|x\rangle, |y\rangle$ を有するこの空間に話を限ることにする．ここで $|y\rangle$ の定義は前と同じである．この表現で $|x\rangle\langle x| = (I+Z)/2 = (I+\hat{z}\cdot\vec{\sigma})/2$, $|\psi\rangle\langle\psi| = (I+\vec{\psi}\cdot\vec{\sigma})/2$ である．ここで $\hat{z} \equiv (0,0,1)$ は $z$ 方向の単位ベクトル，$\vec{\psi} = (2\alpha\beta, 0, (\alpha^2-\beta^2))$ である（これは Bloch ベクトル表現である．4.2 節参照）．簡単な計算により，重要でないグローバル位相因子を除いて

$$\begin{aligned} U(\Delta t) = &\left(\cos^2\left(\frac{\Delta t}{2}\right) - \sin^2\left(\frac{\Delta t}{2}\right)\vec{\psi}\cdot\hat{z}\right) I \\ &-2i\sin\left(\frac{\Delta t}{2}\right)\left(\cos\left(\frac{\Delta t}{2}\right)\frac{\vec{\psi}+\hat{z}}{2} + \sin\left(\frac{\Delta t}{2}\right)\frac{\vec{\psi}\times\hat{z}}{2}\right)\cdot\vec{\sigma}. \end{aligned} \tag{6.25}$$

**演習 6.9:** 式 (6.25) を証明せよ．（ヒント：演習 4.15 を見よ．）

式 (6.25) は Bloch 球上の回転を意味し，その回転軸 $\vec{r}$ は

$$\vec{r} = \cos\left(\frac{\Delta t}{2}\right)\frac{\vec{\psi}+\hat{z}}{2} + \sin\left(\frac{\Delta t}{2}\right)\frac{\vec{\psi}\times\hat{z}}{2} \tag{6.26}$$

で定義され，回転角 $\theta$ は

$$\cos\left(\frac{\theta}{2}\right) = \cos^2\left(\frac{\Delta t}{2}\right) - \sin^2\left(\frac{\Delta t}{2}\right)\vec{\psi}\cdot\hat{z} \tag{6.27}$$

で定義される．この式に $\vec{\psi}\cdot\hat{z} = \alpha^2-\beta^2 = (2/N-1)$ を代入すると簡単化できる：

$$\cos\left(\frac{\theta}{2}\right) = 1 - \frac{2}{N}\sin^2\left(\frac{\Delta t}{2}\right). \tag{6.28}$$

$\vec{\psi}\cdot\vec{r} = \hat{z}\cdot\vec{r}$ なので $|\psi\rangle\langle\psi|$ と $|x\rangle\langle x|$ は Bloch 球上の軸 $\vec{r}$ の回りを回転する同じ円周上にある．以上をまとめると図 6.6 に示すように $U(\Delta t)$ の働きは $U(\Delta t)$ を 1 回適用する度に $|\psi\rangle\langle\psi|$ を軸 $\vec{r}$ の回りに角度 $\theta$ だけ回転する．$|\psi\rangle\langle\psi|$ が解 $|x\rangle\langle x|$ に近づくまで十分回転すると手続きを終了する．最初我々は量子シミュレーションを考えるから $\Delta t$ は小さいと想定したが，式 (6.28) が示すところではスマートに事を運ぶには，回転角 $\theta$ を最大にするために $\Delta t = \pi$ と選ぶ．こうすると $\cos(\theta/2) = 1 - 2/N$ が得られ，これは大きな $N$ に対して $\theta \approx 4/\sqrt{N}$ に相当する．つまり解 $|x\rangle$ を見つけるのに必要なオラクルの呼び出し回数は $O(\sqrt{N})$ となり，元の量子探索アルゴリズムと同じになる．

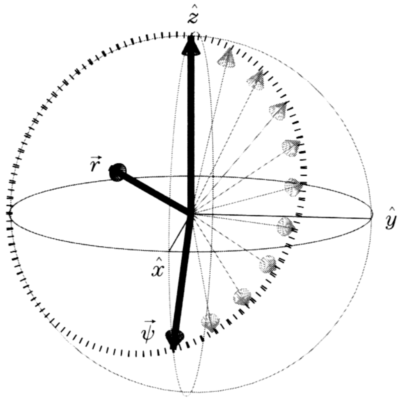



**図 6.6:** 初期状態 $\vec{\psi}$ が回転軸 $\vec{r}$ の回りを回転して最終状態 $\hat{z}$ に近づくことを示す Bloch 球ダイアグラム．

実際もし $\Delta t = \pi$ と選ぶとこの「量子シミュレーション」は元の量子探索アルゴリズムと同じになる．なぜなら量子シミュレーションで適用されたオペレータは $\exp(-i\pi|\psi\rangle\langle\psi|) = I - 2|\psi\rangle\langle\psi|$ と $\exp(-i\pi|x\rangle\langle x|) = I - 2|x\rangle\langle x|$ なので，グローバル位相シフトを除いてこれらは Grover の反復を構成するステップと同一である．こうして見ると量子探索アルゴリズムに対して示した図 6.1 と図 6.2 は，シミュレーションに対する図 6.4 と図 6.5 の回路を $\Delta t = \pi$ の特別な場合に簡単化したものに相当する．

**演習 6.10:** $\Delta t$ を適切に選ぶことにより，$O(\sqrt{N})$ 回の質問を用いて最終状態が**正確に**$|x\rangle$ になる量子探索アルゴリズム — つまり小さな確率でなく確率 1

で働くアルゴリズム — が得られることを示せ.

我々は量子シミュレーションという異なる見地から，量子探索アルゴリズムを再び導いた．なぜこのアプローチがうまく行ったのか？ 他の高速量子アルゴリズムを見つけるのに使えるか？ この問いに確信を持って答えることはできないが，次の二三の考えは興味深いかも知れない．基本的に使われた手続きは次の 4 段階である．

(1) 望ましい入力と量子アルゴリズムからの出力を含めて，解くべき問題を規定する．

(2) 問題を解く Hamiltonian を推定し，実際に役立つことを証明する．

(3) Hamiltonian をシミュレートする手続きを見出す．

(4) シミュレーションのリソースコストを解析する．

これは従来のアプローチと 2 つの点で異なっている： 我々が推定するのは量子回路ではなく Hamiltonian であることと，従来のアプローチに類似のシミュレーションステップがないことである．2 つの違いのうちで最初のものがより重要である．問題を解くために量子回路を規定するには多くの自由度が存在する．この自由度は量子計算の偉大な能力の源である反面，良い回路を見つけるのを難しくしている面がある．これに対して Hamiltonian を規定するのは非常に制約の多い問題であり，したがってその問題の解にはあまり自由度がない．しかしこれらの制約のお陰で，問題を解く効率的な量子アルゴリズムをはるかに容易に見つけることができる．これが量子探索アルゴリズムの場合に起きていることを見てきたことである．多分この方法で他の量子アルゴリズムも見つけられるかも知れないが，それはわからない．確実と思われるのは，「量子シミュレーションとしての量子アルゴリズム」という見方が，量子アルゴリズムの発展を促すもう 1 つの有用な観点である．

**演習 6.11:（多数解を持つ連続量子探索）** 探索問題が $M$ 個の解を持つときに，連続時間の探索問題を解く Hamiltonian を推定せよ．

**演習 6.12:（量子探索の別の Hamiltonian）** 次式を想定する：

$$H = |x\rangle\langle\psi| + |\psi\rangle\langle x|. \tag{6.29}$$

(1) Hamiltonian $H$ に従う時間発展が与えられると，状態 $|\psi\rangle$ から状態 $|x\rangle$ に回転するのに時間 $O(1)$ を要することを示せ．

(2) Hamiltonian $H$ の量子シミュレーションを実行する方法を説明し，シミュレーションで高い確率で解を得るのに必要なオラクルの呼び出し回数を決定せよ．

## 6.3 量子計数

もし $N$ 項目の探索問題であらかじめ解の数 $M$ がわかっていないときに，$M$ をどれだけ早く決定できるか？ 古典コンピュータ上で $M$ を決めるには，明らかにオラクルを $\Theta(N)$ 回参照する．量子コンピュータでは，Grover の反復と量子 Fourier 変換に基づく位相推定テクニック（5 章参照）を組み合わせることにより，古典コンピュータでできるよりはるかに早く解の数を推定できる．これには重要な応用が幾つかある．第 1 にもし解の数を早く推定できると，解も早く見つけられる．解の数がわからなくても，最初に解の数を数えて次に量子探索アルゴリズムを適用して解を見出すことができるからである．第 2 に量子計数により解の数が 0 か 0 でないかに応じて，そもそも解が存在するか否かが決定できる．例えば，探索問題の解の存在によって表現される **NP** 完全問題を解くのにこれが応用できる．

**演習 6.13:** 探索空間から一様かつ独立に $k$ 回サンプルを抽出する計数問題 (数え上げ問題，counting problem) の古典アルゴリズムを考える．オラクル呼び出しの結果を $X_1, \ldots, X_k$，つまり $j$ 番目のオラクル呼び出しが問題の解を示すならば $X_j = 1$，$j$ 番目のオラクル呼び出しが問題の解を示さなければ $X_j = 0$ とする．このアルゴリズムは探索問題の解の数に対して推定値 $S \equiv N \times \sum_j X_j / k$ を返す．$S$ の標準偏差は $\Delta S = \sqrt{M(N-M)/k}$ であることを示せ．すべての値 $M$ に対して精度 $\sqrt{M}$ 以内で $M$ を正確に推定する確率を少なくとも 3/4 にするには，$k = \Omega(N)$ でなければならないことを証明せよ．

**演習 6.14:** ある定数 $c$ とすべての $M$ の値に対して，精度 $c\sqrt{M}$ 以内で $M$ を正

しく推定する確率が少なくとも 3/4 である**任意の**古典的計数アルゴリズムは，オラクルを $\Omega(N)$ 回呼び出さねばならないことを証明せよ．

量子計数 (量子数え上げ，quantum counting) は 5.2 節の位相推定手続きを Grover の反復 $G$ の固有値推定に応用したものであり，これにより探索問題の解の数 $M$ が決定できる．$|a\rangle$ と $|b\rangle$ は，$|\alpha\rangle$ と $|\beta\rangle$ が張る空間における Grover の反復の 2 つの固有ベクトルであるとする．Grover の反復で決まる回転角を $\theta$ とする．式 (6.13) から対応する固有値は $e^{i\theta}$ と $e^{i(2\pi-\theta)}$ である．解析を容易にするために 6.1 節で述べたように探索空間のサイズを $2N$ に広げることによりオラクルを拡大して，$\sin^2(\theta/2) = M/2N$ を保証すると仮定する．

量子計数に使う位相推定回路を図 6.7 に示す．この回路は精度 $m$ ビット，成功確率少なくとも $1-\epsilon$ で $\theta$ で推定する機能を持つ．第 1 レジスタは位相推定アルゴリズム通りに $t \equiv m + \lceil\log(2+1/2\epsilon)\rceil$ 個の q ビットを含み，第 2 レジスタは拡大した探索空間に Grover の反復を実行するのに十分な $n+1$ 個の q ビットを含む．第 2 レジスタの状態は Hadamard 変換によって，すべての可能な入力の等しい重ね合せ $\sum_x |x\rangle$ に初期化する．6.1 節で見たようにこの状態は固有状態 $|a\rangle$ と $|b\rangle$ の重ね合せであり，5.2 節の結果により図 6.7 の回路は精度 $|\Delta\theta| \le 2^{-m}$，確率は少なくとも $1-\epsilon$ で推定値 $\theta$ または $2\pi-\theta$ を与える．さらに推定値 $2\pi-\theta$ は同レベルの精度で推定値 $\theta$ と等価なので，実効的に位相推定アルゴリズムによっ

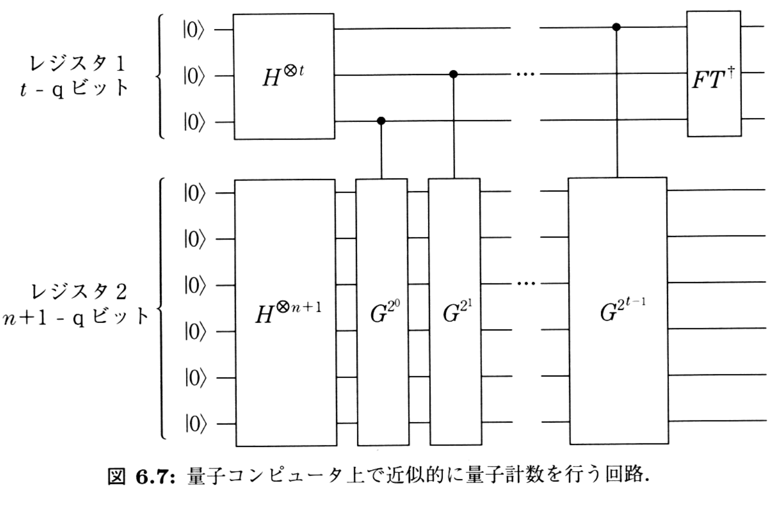



**図 6.7:** 量子コンピュータ上で近似的に量子計数を行う回路．

て精度 $2^{-m}$，確率 $1-\epsilon$ で $\theta$ が決定できる．

式 $\sin^2(\theta/2) = M/2N$ と推定値 $\theta$ を用いると，解の数 $M$ の推定値が得られる．この推定における誤差 $\Delta M$ はどれ位であろうか？

$$\frac{|\Delta M|}{2N} = \left|\sin^2\left(\frac{\theta+\Delta\theta}{2}\right) - \sin^2\left(\frac{\theta}{2}\right)\right| \tag{6.30}$$

$$= \left(\sin\left(\frac{\theta+\Delta\theta}{2}\right) + \sin\left(\frac{\theta}{2}\right)\right) \left|\sin\left(\frac{\theta+\Delta\theta}{2}\right) - \sin\left(\frac{\theta}{2}\right)\right|. \tag{6.31}$$

初歩的な三角関数解析から $|\sin((\theta+\Delta\theta)/2) - \sin(\theta/2)| \leq |\Delta\theta|/2$，$|\sin((\theta+\Delta\theta)/2)| < \sin(\theta/2) + |\Delta\theta|/2$，したがって

$$\frac{|\Delta M|}{2N} < \left(2\sin\left(\frac{\theta}{2}\right) + \frac{|\Delta\theta|}{2}\right)\frac{|\Delta\theta|}{2}. \tag{6.32}$$

$\sin^2(\theta/2) = M/2N$ と $|\Delta\theta| \leq 2^{-m}$ を代入すると，推定値 $M$ の誤差に対する最終の推定値を得る．

$$|\Delta M| < \left(\sqrt{2MN} + \frac{N}{2^{m+1}}\right)2^{-m}. \tag{6.33}$$

例として $m = \lceil n/2 \rceil + 1$ と $\epsilon = 1/6$ を選ぶとする．このとき $t = \lceil n/2 \rceil + 3$，したがってこのアルゴリズムによれば $\Theta(\sqrt{N})$ 回の Grover の反復と $\Theta(\sqrt{N})$ 回のオラクル呼び出しが必要になる．式 (6.33) により精度は $|\Delta M| < \sqrt{M/2} + 1/4 = O(\sqrt{M})$ である．演習 6.14 と比較すると，古典コンピュータで同様の精度を得るには $O(N)$ 回のオラクル呼び出しが必要であった．

実際にいま述べた例はそもそも探索問題の解が存在するかどうか，つまり $M=0$ か $M \neq 0$ かを決めるアルゴリズムとして 2 つの役目を果たす．もし $M=0$ ならば $|\Delta M| < 1/4$ なので，アルゴリズムは少なくとも 5/6 の確率で推定値 0 を与える．逆にもし $M \neq 0$ ならば，少なくとも確率 5/6 で $M$ が 0 に等しくないと推定することが容易に証明できる．

量子計数のもう 1 つの応用は，解の数 $M$ が知られていないときに探索問題の解を**見つける**ことである．6.1 節で述べたように量子探索アルゴリズムを適用するときの困難は，Grover の反復を繰り返す回数 (6.15) が解の数 $M$ を知ることに依存することである．この問題は量子計数アルゴリズムを用いて軽減できる．最初に位相推定を用いて $\theta$ と $M$ を高精度で推定し，次に位相推定で求めた $\theta$ と $M$

の推定値を式 (6.15) に代入して $R$ を決定し，その回数だけ Grover 反復を繰り返すことによって，6.1 節に示したように量子探索アルゴリズムを適用する．この場合の角度誤差はたかだか $\pi/4(1+|\Delta\theta|/\theta)$ であり，前と同じく $m=\lceil n/2\rceil+1$ と選ぶと角度誤差はたかだか $\pi/4\times 3/2=3\pi/8$ となる．これは探索問題の成功確率が少なくとも $\cos^2(3\pi/8)=1/2-1/2\sqrt{2}\approx 0.15$ に相当する．もしこの精度で $\theta$ の推定値を得る確率が前の例のように 5/6 ならば，探索問題の解を得る全確率は $5/6\times\cos^2(3\pi/4)\approx 0.12$ となり，この確率ならば計数・探索の組み合わせ手続きを数回繰り返せば速やかに確率 1 に近づけられる．

## 6.4　NP 完全問題の解の高速化

量子探索は計算量クラス **NP** にある問題（3.2.2 項：第 I 巻参照）の解を高速化するのに使うことができる．すでに 6.1.1 項で素因数分解の高速化法を調べた．ここでは量子探索を使って Hamilton の閉路問題（HC）の解を支援する方法を紹介する．グラフにおける Hamilton の閉路とはグラフ上の全頂点を通る単純な閉路であることを思い出そう．HC 問題は与えられたグラフが Hamilton の閉路を持つかどうかを決定する問題である．この問題は **NP** 完全問題のクラスに属しており，古典コンピュータで解けないと信じられている（が証明されてはいない）．

HC を解く簡単なアルゴリズムでは，順序付けをしたすべての可能な頂点にわたって探索を実行する：

(1) グラフに対する可能な頂点を順序付け $(v_1,\ldots,v_n)$ をする．本質的結果に影響せず解析が容易になるので，重複があっても構わない．

(2) 各順序付けに対してそれがグラフの Hamilton の閉路であるかどうかをチェックする．もし違えば順序付けのチェックを続ける．

探索すべき可能な頂点の順序付けの数は $n^n=2^{n\log n}$ 通りあるので，アルゴリズムは最悪で Hamilton 閉路の性質を $2^{n\log n}$ 回検査する必要がある．一般に **NP** にある問題は実際に同じ方法で解かれる： サイズ $n$ の問題に対して $w(n)$ ビット — $w(n)$ は $n$ の多項式 — で規定される証言 (witness) があるならば，すべての可能な $2^{w(n)}$ 個の証言にわたって探索すると — もし存在するならば — 問題に対する解が現れる．

量子探索アルゴリズムを用いて探索スピードを高めることにより，このアルゴリズムの高速化がはかれる．特に 6.3 節で述べたアルゴリズムを使って，探索問題の解の存在を決定する．$m = \lceil \log n \rceil$ とする．$m$ 個の q ビットブロックがそれぞれ 1 つの頂点の指数を記憶するのに使われるので，アルゴリズムの探索空間は $mn$ 個の q ビット記号列で表される．したがって全 $nm$ - q ビットに対する計算基底状態を $|v_1, \ldots, v_n\rangle$ と書くことができる．ここで各 $|v_i\rangle$ は $m$ - q ビットの適切な記号列で表される．探索アルゴリズムのオラクルは次の変換を行わねばならない：

$$O|v_1, \ldots, v_n\rangle = \begin{cases} |v_1, \ldots, v_n\rangle, \\ \qquad v_1, \ldots, v_n \text{が Hamilton 閉路でない場合} \\ -|v_1, \ldots, v_n\rangle, \\ \qquad v_1, \ldots, v_n \text{が Hamilton 閉路である場合} \end{cases} \tag{6.34}$$

グラフが記述されればこのオラクルは容易に設計・実現できる．グラフ中の Hamilton 閉路を認識する多項式サイズの古典回路を取り上げ，これを変換：$(v_1, \ldots, v_n, q) \to (v_1, \ldots, v_n, q \oplus f(v_1, \ldots, v_n))$ を計算する多項式サイズの可逆回路に変換する．ここでもし $v_1, \ldots, v_n$ が Hamilton の閉路ならば $f(v_1, \ldots, v_n) = 1$，そうでなければ 0 である．対応する回路を量子コンピュータ上で実現すると，状態 $(|0\rangle - |1\rangle)/\sqrt{2})$ から出発して最終 q ビットが所望の変換を与える．ここでは詳細を陽に述べずに主要点だけを記すにとどめる：古典的に多項式数の多数のゲートを使って Hamilton の閉路を認識できるのでその直接的結果として，オラクルは $n$ の多項式数のゲートを必要とする．探索問題の解の存在を決定する探索アルゴリズムの変形（6.3 節）を適用すると，Hamilton の閉路の存在を決めるためにオラクルを $O(2^{mn/2}) = O(2^{n\lceil \log n \rceil/2})$ 回適用することがわかる．もし解が 1 つ存在すると計数・探索の組み合せアルゴリズムを適用して，閉路の例を見つけることは容易であり，次にそれを問題に対する証言として提示する．

まとめると：

- 古典アルゴリズムで Hamilton の閉路が存在するかどうかを決めるには $O(p(n)2^{n\lceil \log n \rceil})$ 回の演算が必要である．ここで多項式因子 $p(n)$ は主としてオラクルの実行に伴う負担分，つまり経路候補が Hamiltonian であるかどうかをチェックするゲート分である．必要なリソースを決める主たる

要因は $2^{n\lceil\log n\rceil}$ のベキ指数である．古典アルゴリズムは決定的，つまり確率 1 で成功する．

- 量子アルゴリズムは $O(p(n)2^{n\lceil\log n\rceil/2})$ 回の演算を使って Hamilton の閉路の存在を決定する．ここでも多項式因子 $p(n)$ は主としてオラクルの実行に伴う負担分である．必要なリソースを決める主たる要因は $2^{n\lceil\log n\rceil}$ のベキ指数である．アルゴリズムには一定の誤り確率（例えば，1/6）があり，これはアルゴリズムを $r$ 回繰り返せば $1/6^r$ に減らせる．
- 量子アルゴリズムは古典アルゴリズムが要求する演算回数に比べて，漸近的に**平方根**の演算回数を必要とする．

## 6.5 構造のないデータベースの量子探索

誰かが 1,000 種類の花の名前を含むリストを渡して，「Perth Rose」がリストの何処にあるか尋ねたとする．もしその花がリストに 1 回だけ含まれていて，しかもリストの配列法が明らかでないならば，「Perth Rose」を探し出すまでに平均 500 回調べる必要がある．そのような**データベース探索**を量子アルゴリズムを使って高速化できないか？ 実際に量子探索アルゴリズムはデータベース探索アルゴリズムとも呼ぶことがあるが，その応用への有効性は限られており，なにがしかの仮定が必要である．本節では量子探索アルゴリズムが構造を持たないデータベースの探索に如何に用いられるか，を**概念的に**見てみる．量子コンピュータが古典的データベースを探索するのに，どんなリソースが必要かを明らかにする．

各々が長さ $l$ ビットを持つ $N \equiv 2^n$ 項目より成るデータベースがあるとする．これらの項目に $d_1, \ldots, d_N$ のラベルを付ける．データベース中の何処に $l$ ビット長の記号列 $s$ があるかを決めたいとする．図 6.8 に示すように，この問題を解く典型的な古典コンピュータは 2 つの部分に分かれている．1 つは**中央演算装置** (CPU) であり，その中にある少数の一時メモリを用いてデータ操作を行う．第 2 の部分は大規模**メモリ**であり $l$ ビット長セルを $2^n$ 個のブロックの記号列としてデータベースを記憶する．メモリはそれ自体のデータを処理できないという意味で，受動的であると仮定する．できることはメモリから CPU にデータを LOAD し，CPU からメモリにデータを STORE し，CPU に一時的に記憶されたデータ

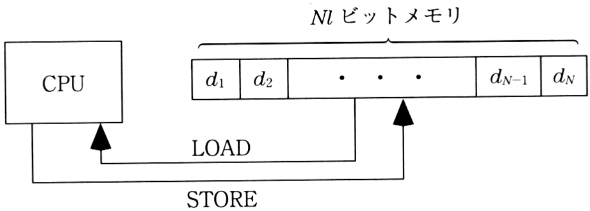



**図 6.8:** 中央演算装置（CPU）とメモリを別々に備えたコンピュータ上での古典的データベース探索．メモリ上で僅か 2 つの演算 — メモリ要素を CPU に LOAD，CPU 演算結果をメモリに STORE — が直接実行される．

を操作することである．もちろん古典コンピュータに異なる設計の考えもあるが，CPU とメモリの分離は通常の一般的なアーキテクチャである．

与えられた記号列 $s$ が構造を持たないデータベースの何処にあるか見つけるための，最も効率の良い古典アルゴリズムは次のようなものである：最初にデータベース要素に付けた $n$ ビットの指標 (index) を CPU 内に作る．CPU は十分大きく $n \equiv \lceil \log N \rceil$ ビットの指標を記憶できるとする．指標は 0 から出発しアルゴリズムを 1 回繰り返す毎に 1 つずつ増加する．各繰り返し毎に指標 $x$ に相当するデータベース項目を CPU に転送し，探している記号列と比較する．もし一致するならばアルゴリズムは指標の値を出力して停止する．一致しなければアルゴリズムは指標を 1 つ増やして探索を続ける．明らかにこのアルゴリズムはメモリから CPU に最悪の場合 $2^n$ 回ロードする必要がある．またこの計算モデルではこれが問題を解く最も効率的なアルゴリズムであることも明らかである．

同様のアルゴリズムを量子コンピュータ上に如何に効率良く実現できるか？ そして量子的高速化ができたとして，そのアルゴリズムはどれだけ有効か？ 最初に高速化が可能であることを示し，その後でアルゴリズムの有効性の議論に戻ることにする．量子コンピュータは古典コンピュータと同様に CPU とメモリの 2 つの部分からなる．CPU には 4 つのレジスタがあると仮定する：

(1) $|0\rangle$ に初期化された $n$ 個の q ビットの「指標」レジスタ

(2) $|s\rangle$ に初期化された $l$ 個の q ビットのレジスタ

(3) $|0\rangle$ に初期化された $l$ 個の q ビットの「データ」レジスタ

(4) $(|0\rangle - |1\rangle)/\sqrt{2}$ に初期化された 1 個の q ビットのレジスタ

メモリ装置は次の 2 つのいずれかの方法で実装される．簡単な方法は各々 $l$ - q ビットセルを $N = 2^n$ 個含み，データベース要素 $|d_x\rangle$ を収容する．第 2 の方法は**古典的**メモリとして実現するもので，各 $l$ ビットセル $N = 2^n$ 個を持ちデータベース要素 $d_x$ を収容する．しかし従来の古典的メモリと異なり，多値の重ね合せをとり得る指標 $x$ によりアドレスできる．この量子指標によってセル値の重ね合せがメモリから LOAD される．メモリへのアクセスは次のように行う：もし CPU の指標レジスタが状態 $|x\rangle$ にありデータレジスタが状態 $|d\rangle$ にあるならば，$x$ 番目のメモリセルの内容 $d_x$ がデータレジスタに加えられる：$|d\rangle \rightarrow |d \oplus d_x\rangle$. ここで和は 2 を法としてビット毎に行う．はじめにこの能力を用いて量子探索を行う方法を調べ，次にそのメモリを物理的に構築する方法を議論する．

量子探索アルゴリズムを実行する重要部分は，メモリ中の $s$ の位置を示す指標の位相を反転するオラクルを実現することである．CPU が状態：

$$|x\rangle|s\rangle|0\rangle\frac{|0\rangle - |1\rangle}{\sqrt{2}} \tag{6.35}$$

にあるとする．LOAD 演算を行うとコンピュータの状態は：

$$|x\rangle|s\rangle|d_x\rangle\frac{|0\rangle - |1\rangle}{\sqrt{2}} \tag{6.36}$$

になる．第 2 と第 3 のレジスタを比較して同じならば第 4 レジスタのビットを反転させ，そうでなければ変化させない．この演算の結果は：

$$|x\rangle|s\rangle|d_x\rangle\frac{|0\rangle - |1\rangle}{\sqrt{2}} \rightarrow \begin{cases} -|x\rangle|s\rangle|d_x\rangle\dfrac{|0\rangle - |1\rangle}{\sqrt{2}}, & d_x = s \\ \quad |x\rangle|s\rangle|d_x\rangle\dfrac{|0\rangle - |1\rangle}{\sqrt{2}}, & d_x \neq s \end{cases} \tag{6.37}$$

次に再び LOAD 演算を行ってデータレジスタを $|0\rangle$ に回復する．したがって，オラクルの全動作によってレジスタ 2, 3, 4 は影響を受けず，レジスタ 1 とのもつれが解ける．したがって全体の効果としてもし $d_s = s$ ならばレジスタの状態が $|x\rangle$ から $-|x\rangle$ に変化し，そうでなければ変化が起きない．オラクルをこのように実行すると量子探索アルゴリズムを使って，古典的に必要な $N$ 回の LOAD 演算に比べて，$O(\sqrt{N})$ 回の LOAD 演算でデータベース内の $s$ の位置を決定できる．

オラクルが重ね合せに対して正しく機能するために，メモリは一見量子力学的である必要があるかに見える．上に見たように実際はある注意を払ったうえで古

典的に実行することが可能であり，このほうが雑音に影響されにい．しかし量子的**アドレス指定**は依然として必要であり，これを行う方法の概念図を図 6.9 に示す．動作原理は次のような手法である．2 進符号化 (binary encoding) した量子指標の状態 — 0 から $(2^n-1)$ を $n$ 個の q ビットで表す — を古典的データベースにアドレスする単項符号化 (unary encoding) — 0 から $(2^n-1)$ を $2^n$ 個の値

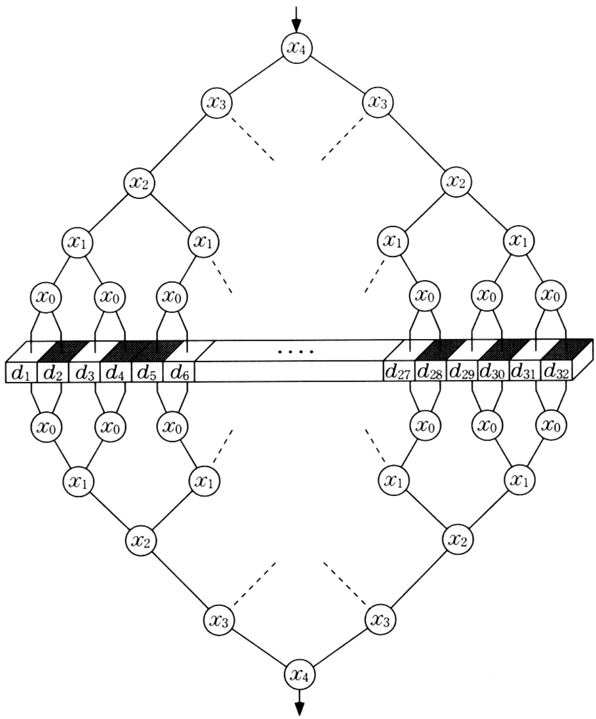



**図 6.9:** 5 個の q ビットの量子アドレス指定法を持つセル数 32 のメモリの概念図．各々の円は中に示した q ビットでアドレス指定されたスイッチを示す．例えば，$|x_4\rangle = |0\rangle$ のとき対応するスイッチは入力 q ビットを左にルートをとり，$|x_4\rangle = |1\rangle$ ならば右にルートをとる．もし $|x_4\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ ならば両ルートの等加重重ね合せをとる．データレジスタの q ビットは木の最上部から入り，下向きルートをたどってデータベースに達してメモリの内容に応じてその値を変える．次に q ビットは逆向きに決まった位置まで戻り，取り出した情報を保持する．物理的にこれを実現するには，例えばデータレジスタ q ビットとして単一光子を用い，非線形干渉計でルートを変える（7 章）．古典的データベースは例えば 1 枚のプラスティック板で「0」は光をそのまま透過（図では白い箱），「1」は光の偏光を 90° 回転する（図では陰付きの箱）．

がとれるプローブ位置の 1 つで表す — に変換し，これを使って古典的データベースにアドレスする．プローブ位置に関係なく，データベースはプローブ内の自由度に変化を及ぼす．次に 2 進数 (binary) から単項数 (unary) への符号化を反転して，データレジスタに希望の内容を渡す．

具体的事例において量子探索アルゴリズムが古典的データベースの探索に有用か？ 2 つの異なる点を指摘できる．第 1 は通常構造を持たないデータベースはない．本節のはじめに議論した花の名前のような簡単なデータベースでもアルファベット順に配列されており，要素数 $N$ のデータベースに対して 2 分探索 (binary search) を用いて $O(\log(N))$ の時間で目的の項目が見つけられる．しかし，あるデータベースにはもっと複雑な構造が要求され，最適な古典的探索のための精巧なテクニックが存在するが，非常に複雑で予期しない検索要求が与えられるとあらかじめ決めた構造は頼りにならず，そのような問題はここで議論した本質的に構造のないデータベース探索問題と見なせる．

第 2 に量子コンピュータが古典的データベースを探索できるためには量子アドレス指定が必要である．ここで述べた方法には $O(N\log N)$ 個の量子スイッチが必要であり，これにはデータベースそれ自体を記憶するのとほぼ同じ量のハードウェアが必要になる．多分何時の日かこのスイッチは古典的メモリ素子と同じくらい単純で安価なものになろうが，もしそうならなければ量子探索を実行する量子コンピュータの構築は，メモリ素子の上に構築された古典計算ハードウェアを用いる場合に比べて，経済的利点がないかも知れない．

これらの考察のもとで量子探索アルゴリズムの主要な用途は，古典的データベース探索にはなりそうにない．むしろその用途は多分前節で述べたように Hamilton の閉路，巡回セールスマン問題，充足可能性問題等の困難な問題の解の探索になるであろう．

## 6.6　最適な探索アルゴリズム

量子コンピュータは探索オラクルを僅か $O(\sqrt{N})$ 回呼び出すだけで，$N$ 項目の探索ができることを示した．次にいかなる量子アルゴリズムも探索オラクルへのアクセス $\Omega(\sqrt{N})$ 回以下ではこのタスクを実行できず，したがってこのアルゴリズムが最適であることを示す．

アルゴリズムが状態 $|\psi\rangle$ から出発するとする．簡単のために探索問題が 1 つの解 $x$ を持つ場合に対する下界を証明する．$x$ を決定するために我々に許されているのは，解 $|x\rangle$ に対して位相シフト $-1$ を与え他のすべての状態を不変に保つオラクル $O_x = I - 2|x\rangle\langle x|$ を適用することである．アルゴリズムは状態 $|\psi\rangle$ から出発してオラクルを正確に $k$ 回適用し，オラクル演算の間にユニタリー演算 $U_1, U_2, \ldots, U_k$ をはさむことを想定する．次式を定義する：

$$|\psi_k^x\rangle \equiv U_k O_x U_{k-1} O_x \ldots U_1 O_x |\psi\rangle \tag{6.38}$$

$$|\psi_k\rangle \equiv U_k U_{k-1} \ldots U_1 |\psi\rangle. \tag{6.39}$$

つまり $|\psi_k\rangle$ はオラクル演算を**行わず**に一連のユニタリー演算 $U_1, U_2, \ldots, U_k$ を行ったときの結果である．$|\psi_0\rangle = |\psi\rangle$ とする．我々のゴールは

$$D_k \equiv \sum_x \|\psi_k^x - \psi_k\|^2 \tag{6.40}$$

なる量の限界を求めることである．ここで式を簡単にするために $|\psi\rangle$ に代えて記号 $\psi$ を使った．直観的に $D_k$ はオラクルを適用しない場合に比べて適用した場合の $k$ **ステップ後のずれ**の尺度である．この量が小さければ全状態 $|\psi_k^x\rangle$ はほぼ同じになり高確率で $x$ を同定できない．証明の戦略は次の 2 つを示すことである：

(1) $O(k^2)$ より早く増大しないという $D_k$ の限界を示す．

(2) $N$ 個の代替を識別できるならば $D_k$ は $\Omega(N)$ でなければならないことを証明する．

これら 2 つを組み合わせると望む下界が得られる．

最初に $D_k \leq 4k^2$ を帰納法で証明する．$k = 0$ に対して $D_k = 0$ なので明らかにこれは正しい．

$$D_{k+1} = \sum_x \|O_x \psi_k^x - \psi_k\|^2 \tag{6.41}$$

$$= \sum_x \|O_x(\psi_k^x - \psi_k) + (O_x - I)\psi_k\|^2. \tag{6.42}$$

を用いる．$\|b+c\|^2 \leq \|b\|^2 + 2\|b\|\|c\| + \|c\|^2$, $b \equiv O_x(\psi_k^x - \psi_k)$, $c \equiv (O_x - I)\psi_k = -2\langle x|\psi_k\rangle|x\rangle$ を適用すると

$$D_{k+1} \leq \sum_x (\|\psi_k^x - \psi_k\|^2 + 4\|\psi_k^x - \psi_k\| \, |\langle x|\psi_k\rangle| + 4|\langle \psi_k|x\rangle|^2). \tag{6.43}$$

右辺第 2 項に Cauchy-Schwarz の不等式を適用して，$\sum_x |\langle x|\psi_k\rangle|^2 = 1$ を用いると

$$D_{k+1} \le D_k + 4\Big(\sum_x \|\psi_k^x - \psi_k\|^2\Big)^{\frac{1}{2}}\Big(\sum_{x'} |\langle\psi_k|x'\rangle|^2\Big)^{\frac{1}{2}} + 4 \tag{6.44}$$

$$\le D_k + 4\sqrt{D_k} + 4. \tag{6.45}$$

帰納法の仮定 $D_k \le 4k^2$ より

$$D_{k+1} \le 4k^2 + 8k + 4 = 4(k+1)^2. \tag{6.46}$$

よって帰納法により証明された．

証明を完成させるには，$D_k$ が $\Omega(N)$ のときにのみ成功確率が高くなり得ることを示す必要がある．すべての $x$ に対して $|\langle x|\psi_k^x\rangle|^2 \ge 1/2$ とすると，観測により探索問題の解を得る確率は少なくとも 1/2 である．$|x\rangle$ を $e^{i\theta}|x\rangle$ で置き換えても成功確率は変化しないので，$\langle x|\psi_k^x\rangle = |\langle x|\psi_k^x\rangle|$ と仮定しても一般性を失わない．

$$\|\psi_k^x - x\|^2 = 2 - 2|\langle x|\psi_k^x\rangle| \le 2 - \sqrt{2}. \tag{6.47}$$

$E_k \equiv \sum_x \|\psi_k^x - x\|^2$ と定義すると $E_k \le (2-\sqrt{2})N$ が得られる．いよいよ $D_k$ が $\Omega(N)$ であることを証明する段階になった．$F_k \equiv \sum_k \|x - \psi_k\|^2$ と定義すると

$$D_k = \sum_x \|(\psi_k^x - x) + (x - \psi_k)\|^2 \tag{6.48}$$

$$\ge \sum_x \|\psi_k^x - x\|^2 - 2\sum_x \|\psi_k^x - x\|\,\|x - \psi_k\| + \sum_x \|x - \psi_k\|^2 \tag{6.49}$$

$$= E_k + F_k - 2\sum_x \|\psi_k^x - x\|\,\|x - \psi_k\|. \tag{6.50}$$

Cauchy-Schwarz の不等式を適用すると，$\sum_x \|\psi_k^x - x\|\,\|x - \psi_k\| \le \sqrt{E_k F_k}$ なので

$$D_k \ge E_k + F_k - 2\sqrt{E_k F_k} = (\sqrt{E_k} - \sqrt{F_k})^2. \tag{6.51}$$

演習 6.15 で $F_k \ge 2N - 2\sqrt{N}$ を示す．これと $E_k \le (2-\sqrt{2})N$ を組み合わせると，十分大きな $N$ に対して $D_k \ge cN$ を得る．ここで $c$ は $(\sqrt{2} - \sqrt{2-\sqrt{2}})^2 \approx 0.42$ より小さな任意の定数である．$D_k \le 4k^2$ だからこれは次式を意味する．

$$k \ge \sqrt{cN/4}. \tag{6.52}$$

まとめると，探索問題の解を見出す成功確率少なくとも 1/2 を達成するには，オラクルを $\Omega(\sqrt{N})$ 回呼び出さねばならない．

**演習 6.15:** Cauchy-Schwarz の不等式を用いて，任意の正規化状態ベクトル $|\psi\rangle$ と $N$ 個の正規直交基底ベクトル集合 $|x\rangle$ に対して次式を示せ．

$$\sum_x \|\psi - x\|^2 \geq 2N - 2\sqrt{N}. \tag{6.53}$$

**演習 6.16:** $x$ のすべての値に対してではなく，$x$ の可能な値に対して一様に平均を取ったときに，誤り確率が 1/2 以下になるということだけを要求するとする．このときも探索問題を解くのに求められるオラクル呼び出しは $O(\sqrt{N})$ であることを示せ．

量子探索アルゴリズムが本質的に最適であるというこの結果は感激的でもあり，失望するものでもある．感激する理由は少なくともこの問題に対して我々は量子力学の奥深さを完全に理解したからであり，これ以上の改善はできない．失望する理由は量子探索アルゴリズムによって平方根以上の高速化が提供されると望んでいたからである．先験的に望んでいた夢は，$N$ 項目の探索空間をオラクル呼び出し $O(\log N)$ 回で探索できればよいということであった．もしそのようなアルゴリズムが存在するならば，量子コンピュータ上で **NP** 完全問題が効率良く解けることになったであろう．なぜなら $2^{w(n)}$ のすべての可能な証言 — 多項式 $w(n)$ は証言の長さのビット数 — をほぼ $w(n)$ 回のオラクル呼び出しで探索できるからである．不幸にしてそのようなアルゴリズムは可能でない．これは探索ベースの素朴な **NP** 完全問題攻略法の失敗を保証することを示すので，アルゴリズム志願者にとって役立つ情報である．

敢えて個人的意見をいうと，**NP** 完全問題の困難さの本質的理由はその探索空間が構造を持たないことと，（多項式因子を無視すると）そのような問題が解ける最善の方法は，探索法の採用であると多くの研究者が信じているのが認められる．もしこの見解をとるならば，量子コンピュータで効率的に解ける問題のクラス **BQP** は **NP** 完全問題を含まないので，これは量子計算にとって悪いニュースである．もちろんこれは単なる意見であって，**NP** 完全問題が何か未知の構造を持っていて量子コンピュータ上で効率良く解けるとか，古典コンピュータでも

解けるという可能性も残っている．この点を示す良い例が，困難さの点で **P** と **NP** 完全問題の中間に位置する，クラス **NPI** にあると広く信じられていた素因数分解問題である．素因数分解問題の効率的量子力学解が見つかった鍵は問題内に「隠れ」構造— 位数発見に縮約することにより現れた構造 — を利用したからである．量子力学的にはこの構造により効率的素因数分解アルゴリズムが強化されたが，この目覚ましい構造が現れてもこれを使って効率の良い素因数分解の古典アルゴリズムを開発することが可能だとはわかっていない！　グラフ同形問題のような **NPI** にあると疑われている問題や，**NP** 完全問題それ自体の他の問題にも，多分同様の構造が潜んでいるかも知れない．

**演習 6.17:（多数解に対する最適性）** 探索問題が $M$ 個の解を持つとする．解を見出すのにオラクル呼び出しを $O(\sqrt{N/M})$ 回行う必要があることを示せ．

## 6.7　ブラックボックス アルゴリズムの限界

本章の最後に量子計算能力の限界を洞察する，量子探索アルゴリズムの一般化について述べる．本章のはじめに探索問題は関数 $f:\ \{0,1\}^n \rightarrow \{0,1\}$ が $f(x)=1$ と評価するような $n$ ビットの整数 $x$ を見つけることであると述べた．これに関連するのは $f(x)=1$ を満たす $x$ が存在するかどうかという**決定問題** (decision problem) である．この決定問題を解くことは同様に困難であり，Boole 関数 $F(X)=X_0 \vee X_1 \vee \cdots \vee X_{N-1}$ を計算することとして表現できる．ここで $\vee$ は 2 進数の OR 演算，$X_k \equiv f(k)$，$X$ は集合 $\{X_0,\ X_1,\ldots,\ X_{N-1}\}$ を表す．一般に OR 以外の何か他の関数を計算したいときがあるかも知れない．例えば $F(X)$ は AND，PARITY（2 を法とする和），MAJORITY（$X_k=1$ がそれ以外より多いときにのみ $F(X)=1$）であってもよい．一般に $F$ は任意の Boole 関数と考えてよい．$f$ のオラクルが与えられたとき，古典的であれ量子的であれ，コンピュータが（質問回数で数えて）如何に早くこれらの関数を計算できるか？

関数 $f$ に関する知識を何も持たずに，そのような質問に答えるのは難しそうに見えるが，オラクルがそのタスクを実行する方法が認めらており，複雑さがオラクルへの質問要求回数で測られるこの「ブラックボックス」モデルを使って，非常に多くのことが実際に決定できる．前節の探索アルゴリズム解析で，このよう

な問題を扱う 1 つの方法を示したが，質問の計算量の解を取り扱うもっと強力な解法に，**多項式の方法** (method of polynomials) がある．これについて簡単に述べる．

幾つかの便利な定義から始める．決定性の質問の計算量 $D(F)$ とは古典コンピュータが $F$ を確定的に計算するために実行すべきオラクル呼び出しの最小回数である．それに対応する量子的な計算量 $Q_E(F)$ は量子コンピュータが $F$ を確定的に計算するために実行すべきオラクル呼び出しの最小回数である．量子コンピュータはその性質として確率的出力を与えるので，より興味ある量は有界誤り計算量 $Q_2(F)$ である．これは量子コンピュータが少なくとも 2/3 の確率で $F$ に等しい出力を与えるに要する最小のオラクル呼び出し回数である（2/3 は任意の数である — 繰り返しによって 1 に高めるために，1/2 から有限量だけ大きな下界を持つ確率であればよい）．関連した尺度はゼロ誤り計算量 $Q_0(F)$ であり，これは量子コンピュータが確定的にあるいは決定的でない結果を認めて 1/2 以下の確率で，$F$ に等しい出力を与えるに要するオラクル呼び出しの最小回数である．これらの下界はすべて任意のオラクル関数 $f$（つまり任意の $F$ への入力 $X$）に対して成立する．$Q_2(F) \leq Q_0(F) \leq Q_E(F) \leq D(F) \leq N$ であることに留意する．

多項式の方法は Boole 関数を**表現**する（**実数**に関する）最小次数の多重線形多項式 (multilinear polynomial) の性質に基づいている．ここで考えるすべての多項式は $X_k \in \{0,1\}$ の関数であり，したがって $X_k^2 = X_k$ なので多重線形である．もしすべての $X \in \{0,1\}^N$ に対して $p(X) = F(X)$ ならば，多項式 $p : \mathbf{R}^N \to \mathbf{R}$ は $F$ を表すという（ここで $\mathbf{R}$ は実数を表す）．多項式 $p$ に対して次のような適切な候補を明示的に作れるので，そのような多項式は常に存在する：

$$p(X) = \sum_{Y \in \{0,1\}^N} F(Y) \prod_{k=0}^{N-1} \Big[1 - (Y_k - X_k)^2\Big]. \tag{6.54}$$

最小次数 $p$ が一意に決まることは演習 6.18 で読者に委ねる．$F$ に対するそのような表現の最小次数 $\deg(F)$ は，$F$ の複雑さを表す便利な尺度である．例えば，deg(OR), deg(AND), deg(PARITY) はすべて $N$ に等しいことが知られている．実際たいていの関数の次数は $N$ に等しいことがわかっている．さらに次式が証明されている：

$$D(F) \leq 2 \deg(F)^4. \tag{6.55}$$

この結果はたいていの Boole 関数を計算する際に古典的な決定性計算の性能に対する上界を与える．この概念を拡張して，すべての $X \in \{0,1\}^N$ に対して多項式が $|p(X) - F(X)| \le 1/3$ を満たすならば $p$ **は** $F$ **を近似する**といい，$\widetilde{\deg}(F)$ はそのような近似多項式の最小次数を表す．これは確率的な古典計算の重要な尺度であり，これから調べるように量子計算でも同様である．$\widetilde{\deg}(\mathrm{PARITY}) = N$ であることがわかっており

$$\widetilde{\deg}(\mathrm{OR}) \in \Theta(\sqrt{N}) \quad \text{および} \quad \widetilde{\deg}(\mathrm{AND}) \in \Theta(\sqrt{N}), \tag{6.56}$$

および

$$D(F) \le 216\, \widetilde{\deg}(\mathrm{F})^6. \tag{6.57}$$

式 (6.55) と式 (6.57) の限界は本書の執筆時点で最もよく知られているものに過ぎない．その証明は本書の範囲外であるが，これらに関する詳しい情報は「歴史と参考資料」に見出せる．よりタイトな限界も可能であるが我々の目的にはこれで十分である．

**演習 6.18:** Boole 関数 $F(X)$ を表す最小次数の多項式は一意であることを証明せよ．

**演習 6.19:** $P(X) = 1 - (1 - X_0)(1 - X_1) \ldots (1 - X_{N-1})$ は OR を表現することを示せ．

量子アルゴリズムの結果を述べるときには多項式が自然に出てくる．オラクル $O$ に $T$ 回質問をする量子アルゴリズム $Q$ の出力を次のように書く：

$$\sum_{k=0}^{2^n-1} c_k |k\rangle. \tag{6.58}$$

振幅 $c_k$ は変数 $X_0$, $X_1, \ldots,$ $X_{N-1}$ に関するたかだか次数 $T$ の多項式であることを示そう．任意の $Q$ は図 6.10 に示す量子回路で実現できる．最初のオラクル呼び出しの直前にある状態 $|\psi_0\rangle$ は次のように書ける：

$$|\psi_0\rangle = \sum_{ij} \Big( a_{i0j} |i\rangle|0\rangle + a_{i1j} |i\rangle|1\rangle \Big) |j\rangle, \tag{6.59}$$

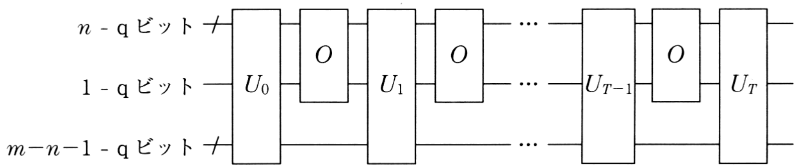



**図 6.10:** オラクル $O$ に $T$ 回質問をする量子アルゴリズムの一般的量子回路．$U_0$, $U_1, \dots,$ $U_T$ は $m$ 個の q ビットに働く任意のユニタリー変換であり，オラクルは $n+1$ 個の q ビットに作用する．

ここで最初のラベルは $Q$ の中で使われる $n$ - q ビットのオラクル質問，次のラベルは結果を残しておく単一 q ビット，最後のラベルは $m-n-1$ 個の作業 q ビットに対応する．オラクル呼び出し後の状態は：

$$|\psi_1\rangle = \sum_{ij}\Big(a_{i0j}|i\rangle|X_i\rangle + a_{i1j}|i\rangle|X_i \oplus 1\rangle\Big)|j\rangle. \tag{6.60}$$

しかし $X_i$ は 0 か 1 なのでこれを書き換えると

$$\begin{aligned}|\psi_1\rangle = \sum_{ij}\big[&\left((1-X_i)a_{i0j} + X_i a_{i1j}\right)|i0\rangle \\ &+\left((1-X_i)a_{i1j} + X_i a_{i0j}\right)|i1\rangle\big]|j\rangle.\end{aligned} \tag{6.61}$$

$|\psi_0\rangle$ において計算基底状態の振幅は $X$ に関して次数 0，$|\psi_1\rangle$ においては次数 1（$X$ に対して線形）である．重要なことはオラクル質問の前か後で $Q$ が実行する任意のユニタリー演算は，これら多項式の次数を変えることができないが，各オラクル呼び出しは次数をたかだか 1 だけ増加させることができる．したがって $T$ 回の質問後では振幅はたかだか次数 $T$ の多項式になる．さらに計算基底で最終結果 (6.58) を測定すると，確率 $P_k(X) = |c_k|^2$ で結果 $k$ を生じ，これはたかだか次数 $2T$ を有する $X$ の実数値多項式である．

このアルゴリズムから出力 1 を得る全確率 $P(X)$ は，多項式 $P_k(X)$ のある部分集合に関する総和であり，したがって，これもたかだか $2T$ の次数を持つ．$Q$ が正しい答を確実に与えるときは $P(X) = F(X)$ でなければならないので，$\deg(F) \le 2T$ であり，したがって

$$Q_E(F) \geq \frac{\deg(F)}{2}. \tag{6.62}$$

$Q$ が有界な誤り確率で答を与える場合は $P(X)$ が $F(X)$ を近似し，したがって $\widetilde{\deg}(F) \leq 2T$，これから

$$Q_2(F) \geq \frac{\widetilde{\deg}(F)}{2} \tag{6.63}$$

が導ける．(6.55) と (6.62) を組み合わせると

$$Q_E(F) \geq \left[\frac{D(F)}{32}\right]^{1/4}. \tag{6.64}$$

同様に (6.57) と (6.63) を組み合わせると

$$Q_2(F) \geq \left[\frac{D(F)}{13824}\right]^{1/6}. \tag{6.65}$$

この意味するところは，ブラックボックスを使って Boole 関数を計算する際に量子コンピュータは古典コンピュータに比べて**最良でも**多項式の高速化しかもたらさない — しかもそれすら（たいていの関数に対して $\deg(F)$ は $\Omega(N)$ であるから）一般に可能ではない．他方で $F = \mathrm{OR}$ に対して $D(F) = N$，確率的な古典的問い合せの計算量は $R(F) \in \Theta(N)$ であることがわかっている．一方 (6.63) と (6.56) を組み合わせて量子探索アルゴリズムの性能を考えると，$Q_2(F) \in \Theta(\sqrt{N})$ が示される．この平方根の高速化は量子探索アルゴリズムが達成したそのものであり，多項式の方法は多分この結果がもう少し広いクラスの問題に一般化できることを示している．しかしブラックボックスのオラクル関数 $f$ の**構造**に関する特別な情報がなければ，古典アルゴリズムに対して指数関数的な高速化は不可能である．

**演習 6.20:** 誤りなしに OR を計算する量子回路の出力から OR 関数を表現する多項式を作って，$Q_0(\mathrm{OR}) \geq N$ を示せ．

**問題 6.1:**（**最小値を見つける**）　6.5 節で示したように $x_1, \ldots, x_N$ はメモリに蓄えられた数のデータベースとする．リスト中の最小の要素を少なくとも確率 1/2 で見出すために，量子コンピュータに要求されるメモリアクセス回数はわずか $O(\log(N)\sqrt{N})$ であることを示せ．

**問題 6.2:（量子探索の一般化）** $|\psi\rangle$ を量子状態として，$U_{|\psi\rangle} \equiv I - 2|\psi\rangle\langle\psi|$ を定義する．つまり $U_{|\psi\rangle}$ は状態 $|\psi\rangle$ に対して位相 $-1$ を与え，$|\psi\rangle$ に直交する状態は不変に保つ．

(1) $U|0\rangle^{\otimes n} = |\psi\rangle$ なるユニタリーオペレータ $U$ を実行する量子回路があるとする．$U_{|\psi\rangle}$ を実現する方法を説明せよ．

(2) $|\psi_1\rangle = |1\rangle$, $|\psi_2\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$, $|\psi_3\rangle = (|0\rangle - i|1\rangle)/\sqrt{2}$ とする．未知のオラクル $O$ が集合 $U_{|\psi_1\rangle}$, $U_{|\psi_2\rangle}$, $U_{|\psi_3\rangle}$ から選ばれるとする．このオラクルを **1 回**適用するだけでオラクルを同定する量子アルゴリズムを与えよ．（ヒント：超高密度符号化を用いよ．）

(3) **研究：**一般に $k$ 個の状態 $|\psi_1\rangle, \ldots, |\psi_k\rangle$ と，集合 $U_{|\psi_1\rangle}, \ldots, U_{|\psi_k\rangle}$ から選んだ未知のオラクル $O$ が与えられたとき，高確率でオラクルを同定するにはオラクルを何回適用する必要があるか？

**問題 6.3:（データベース検索）** $n$ - q ビットの質問（と 1 - q ビットのメモ用紙）$|k, y\rangle$ が与えられたときに，$|k, y \oplus X_k\rangle$ を返す量子オラクルがあるとする．このとき $N/2 + \sqrt{N}$ 回の質問のみを用いて高確率で $X$ の $N = 2^n$ ビットすべてが得られることを示せ．これは任意の $F$ に対して一般的上界が $Q_2 \le N/2 + \sqrt{N}$ であることを意味する．

**問題 6.4:（量子探索と暗号）** 量子探索は潜在的に暗号鍵探索の高速化に使える．復号化のためのすべての可能な鍵の空間を探索し，それぞれの鍵を試行して復号化されたメッセージが「意味」をなすかを検査するというアイディアを考える．このアイディアは Vernam 暗号（12.6 節：第 III 巻）に対して働かない理由を説明せよ．どのようなときに DES のような暗号システムに働くか？（DES の説明は例えば [MvOV96] または [Sch96a] を参照．）

**6 章のまとめ: 量子探索アルゴリズム**

- **量子探索アルゴリズム：** $N = 2^n$ の可能性の中から $M$ 個の解を探索する問題に対して，$\sum_x |x\rangle$ を用意して $G \equiv H^{\otimes n} U H^{\otimes n} O$ を全部で $O(\sqrt{N/M})$ 回繰り返す．ここで $O$ は $x$ が解ならば $|x\rangle \to -|x\rangle$，そうでなければ変化させない探索オラクル，$U$ は $|0\rangle \to -|0\rangle$ で他の全計算基底は変化させない．測定すると探索問題の解が高確率で得られる．

- **量子計数アルゴリズム：** 探索問題が未知の数 $M$ 個の解を持つとする．$G$ は固有値 $\exp(\pm i\theta)$ を持つ．ここで $\sin^2(\theta/2) = M/N$ である．Fourier 変換に基づく位相推定手続きにより，オラクルを $O(\sqrt{N})$ 回適用すると高確率で $M$ を推定できる．これに対して量子計数は与えられた探索問題が解を持つかどうかを決定することができて，前もって解の数がわかっていなくても，もしあればそれを見つける．
- **多項式の限界：**（部分関数 (partial function) や「約束」問題 (promise problem) と異なり）全体関数 (total function) $F$ の評価として記述される問題に対して，量子アルゴリズムは古典アルゴリズムより多項式以上の高速化はできない．具体的には $Q_2(F) \geq [D(F)/13824]^{1/6}$ である．さらに量子探索の性能は最適であって，$\Theta(\sqrt{N})$ である．

## 歴史と参考資料

量子探索アルゴリズムとその発展は Grover [Gro96] [Gro97] による．Boyer, Brassard, Høyer, Tapp は影響力のある論文 [BBHT98] を書き，解の数 $M$ が 1 より大きい場合に量子探索アルゴリズムを発展させ，量子計数アルゴリズムの概略を示した．後者はその後 Brassard, Høyer, Tapp [BHT98] により詳細に発展され，Mosca [Mos98] により位相推定の観点から発展された．Grover 反復を 2 回の反射の積で理解することは Aharonov の解説 [Aha99b] で指摘された．連続時間 Hamiltonian (6.18) は 6.2 節と少し異なる観点から Farhi と Gutmann[FG98] が最初に調べた．Grover のアルゴリズムが可能な最良のオラクルベースの探索アルゴリズムであることは Bennett, Bernstein, Brassard, Vazirani [BBBV97] により証明された．我々が示した証明は Boyer, Brassard, Høyer, Tapp [BBHT98] に基づいている．Zalka [Zal99] はこれらの証明を洗練し量子探索アルゴリズムが漸近的に正確に最適であることを示した．

量子アルゴリズムの能力の限界を示す多項式の方法を量子計算に導入したのは Beals, Buhrman, Cleve, Mosca, de Wolf [BBC+98] である．Mosca の博士論文 [Mos99] にも優れた議論が載っており 6.7 節の議論はこれに基づいている．こ

の節には証明なしに多くの結果を引用したが，その引用元は次の通りである．式 (6.55) は [BBC+98] から引用したが，それ以外は出版されていない．式 (6.56) は Paturi[Pat92] による定理から導き，式 (6.57) は [BBC+98] で導かれている．式 (6.65) より良い限界が [BBC+98] に与えられているが，そこでは本書の範囲外の**ブロック感度** (block sensitivity) のような概念を使っている．量子ブラックボックス アルゴリズム の限界に対して，もつれに基づく議論を用いた全く異なるアプローチは Ambainis [Amb00] により示された．

問題 6.1 は Dürr と Høyer [DH96] に，問題 6.3 は van Dam [van98a] によっている．

# 第7章　量子コンピュータ：物理的実現法

未来のコンピュータは 1.5 トン以下の重さになるであろう．
— Popular Mechanics 誌，科学の間断なき進歩を予測して，1949 年．

世界市場のコンピュータ需要は多分 5 台はあると思う．
— Thomas Watson，IBM 会長，1943 年

我々は量子情報処理機械が実際に自然界に実現できると信じているので，量子計算と量子情報は基本的興味が持てる分野である．そうでなければこの分野は数学的興味に終わってしまう！ それにもかかわらず量子回路，アルゴリズムおよび通信システムを実験で実現することは非常に困難であるのがわかる．本章では量子情報処理デバイスとシステムを物理的に実現する指導原理とモデルシステムを追求する．

7.1 節では量子コンピュータの物理的実現法を選択する際の長所短所を概観する．この議論に基づき 7.2 節で量子コンピュータを実験で実現するときの十分条件を詳細に展望する．7.3 節から 7.7 節における一連のケーススタディで，5 つの異なる物理システムモデルを例にあげてこれらの条件を示す：つまり単純な調和振動子，光子と非線形光学媒質，共振器量子電気力学デバイス，イオントラップ，分子の核磁気共鳴である．個々のシステムに対して物理的装置，ダイナミクスを支配する Hamiltonian，量子計算を行うシステム制御手段，および主要な欠点を簡単に述べる．各々のシステムはそれ自体で 1 つの分野を構成しており，これらシステムの物理を深く述べるのは本書の範囲を越えるので差し控える．その代わりに実験的課題と理論的可能性の両方が理解できるように，量子計算と量子情報

に関連する概念をまとめる．他方で量子情報の観点からこれらのシステムを解析することにより，重要な物理学が驚くほど簡単に導かれるので，新鮮で洞察力に富む見通しが得られるであろう．本章最後の7.8節でこの分野にとって興味がある他の物理システムの分野 — 量子ドット，超伝導ゲート，および半導体中のスピン— について議論する．読者が各物理的実現法のハイライトを把握できるように各節の最後にまとめを付した．

## 7.1　指導原理

量子コンピュータを構築するうえでの実験的要請は何か？ 理論上の基本単位は量子ビット — 2準位量子システム— である．1.5節（第I巻）でなぜqビットが自然界に存在すると信じられ，それがどんな物理的形態をとるかについて簡単に述べた．量子コンピュータを実現するために，qビットに（量子的性質を保った）何かロバストな物理的表現を与えると同時に，望み通りに時間発展できるシステムを選ばなければならない．さらにqビットをある特定の初期状態に設定できて，システムの最終出力を測定できる必要がある．

実験的に実現するうえの課題は，これら基本的要求が部分的にしか満たされない場合が多いことである．コインには2つの状態があるので良いビットになるが，長時間（「表」と「裏」の）重ね合せ状態をとることはできないので，まずいqビットである．単一核スピンは外部磁場に平行と反平行の重ね合せが長時間 — 数日も — 続くので非常に良いqビットである．しかし外部との結合が弱く単一核スピンの方向の測定が困難なので，核スピンから量子コンピュータを構築するのが困難である．一般にこれらの制約は相反している：量子コンピュータはその量子状態を保つために孤立していなければならないが，同時に計算を行い結果を読み出すために，そのqビットにアクセスできなければならない．現実に実現するにはこれら制約の微妙な妥協点を見出して，**如何に**量子コンピュータを作るかではなく，**如何に良い**量子コンピュータを作るかを問題にしなければならない．

量子情報を取り扱うのにどんな物理システムが潜在的に良い候補か？ 特定の量子コンピュータ実現法の利点を理解する鍵は**量子雑音**（**コヒーレンス劣化**(デコヒーレンス，decoherence) とも呼ぶ）の概念であり，8章の主題とする．これはシステムの望ましい時間発展を妨げるプロセスである．この理由は可能な最も

長い量子計算の長さが，システムが量子力学的にコヒーレントである時間 $\tau_Q$ と，(少なくとも 2 個の q ビットを含む) 基本的ユニタリー変換を実行する時間 $\tau_{op}$ の比でほぼ与えられるからである．多くのシステムではこれら 2 つの時間は，両方ともシステムと外界との結合の強さで決まるので，実際には互いに関連している．それにもかかわらず $\lambda = \tau_{op}/\tau_Q$ は図 7.1 に示すように驚くほど広い範囲に広がっている．

| システム | $\tau_Q$ | $\tau_{op}$ | $n_{op} = \lambda^{-1}$ |
|---|---|---|---|
| 核スピン | $10^{-2} - 10^{8}$ | $10^{-3} - 10^{-6}$ | $10^{5} - 10^{14}$ |
| 電子スピン | $10^{-3}$ | $10^{-7}$ | $10^{4}$ |
| イオントラップ ($In^{+}$ ) | $10^{-1}$ | $10^{-14}$ | $10^{13}$ |
| 電子 — 金 | $10^{-8}$ | $10^{-14}$ | $10^{6}$ |
| 電子 — GaAs | $10^{-10}$ | $10^{-13}$ | $10^{3}$ |
| 量子ドット | $10^{-6}$ | $10^{-9}$ | $10^{3}$ |
| 光共振器 | $10^{-5}$ | $10^{-14}$ | $10^{9}$ |
| マイクロ波共振器 | $10^{0}$ | $10^{-4}$ | $10^{4}$ |

**図 7.1:** 量子ビットの相互作用システムを物理的に実現する候補に関するコヒーレンス時間 $\tau_Q$ (秒)，演算時間 $\tau_{op}$ (秒) および最大演算回数 $n_{op} = \lambda^{-1} = \tau_Q/\tau_{op}$ の大まかな見積もり．本表の項目数は多いが，基本的に異なる 3 つの q ビット表現があげられる：つまりスピン，電荷および光子である．イオントラップは閉じ込められたイオン中の電子スピンや核スピンの反転に対応する，微細構造または超微細構造の遷移を利用する (7.6 節参照)．金や GaAs，あるいは量子ドット中の電子に対する推定値は電荷利用の代表として示したもので，電極やその他の閉じ込め領域が電子を含むかどうかで動作する．光やマイクロ波共振器中の異なるモードに分布する (周波数 数 GHz から数百 THz の) 光子は q ビットを表す．本表は広範囲の可能性を展望するために示したものであり，これらの値は割引して受け取るべきである．

この見積もりは量子情報処理機械を実現する異なる物理媒体の利点に関して見通しを与えるが，実際に実現するに当たっては雑音や不完全さの原因が数多く存在する．例えば，原子の 2 準位で表現される q ビットを取り扱い，光を使って準位間遷移を起こさせるとすると，ある確率で他準位への遷移も生じてしまう．これが起きるとシステムは q ビットを定義する 2 準位から外れてしまうので，これも雑音過程と考えられる．一般に (量子) 情報の損失を引き起こすものはすべて雑音過程であり，量子雑音の理論については 8 章でもっと深く議論する．

## 7.2　量子計算の条件

前節の最初に述べた量子計算の4つの基本的要求条件に戻って詳しく議論する．この条件とは次の能力である：

(1) 量子情報をロバストに表現できる．

(2) 普遍的ユニタリー変換の集まりを実行できる．

(3) 信頼できる初期状態を準備できる．

(4) 出力結果を測定できる．

### 7.2.1　量子情報の表現

量子計算は量子状態の変換に基づいている．量子ビットは2準位の量子システムであり，量子コンピュータの最も単純な構成ブロックとして，状態対とその物理的実体に便利なラベルを付ける．例えばスピン3/2の粒子の4状態 $|m=+3/2\rangle$, $|m=+1/2\rangle$, $|m=-1/2\rangle$, $|m=-3/2\rangle$ は2つのqビットを表すのに使える．

計算に重要な実体は，アクセスできる状態の集合が**有限**でなければならない．1次元直線上の粒子の位置 $x$ は，量子状態 $|x\rangle$ やその重ね合せ状態 $\sum_x c_x|x\rangle$ にあるとしても，一般に計算に適した状態の集合と言えない．この理由は $x$ はとり得る値が連続値域にあるためHilbert空間サイズが無限大であり，雑音がない場合の情報容量が無限大となる．例えば，完全な世界においてShakespeareの全文が2進小数で表された無限個数の数字 $x=0.010111011001\ldots$ で記憶され（そして読み出せ）ることになる．これは明らかに非現実的である．現実には雑音により識別できる状態数が有限個数に減少する．

実際に生じるコヒーレンス劣化を最小にするために，一般に何かの対称性により状態空間が有限になることが望ましい．例えばスピン1/2の粒子は状態 $|\uparrow\rangle$ と $|\downarrow\rangle$ が張るHilbert空間に存在する．スピン状態がこの2次元空間以外には存在し得ないため十分に孤立化していると，理想に近い量子ビットになる．

もし表現の選択がうまくなければコヒーレンス劣化が生じる．例えばコラム7.1で述べるように，2つの束縛状態だけを含む深さを持つ有限な方形井戸中の粒子は，束縛状態から非束縛の連続状態への遷移が可能なので，優れた量子ビットにならない．qビットの重ね合せ状態が破壊されてコヒーレンス劣化が生じるのである．1個のqビットに対する性能指数は任意の重ね合せ状態の最小の寿命で与

えられる．スピン状態や原子システムに使われる良い尺度は $(|0\rangle + |1\rangle)/\sqrt{2}$ のような状態の「横」緩和時間 (transverse relaxation time) $T_2$ である．上のエネルギー状態 $|1\rangle$ の「縦」緩和時間 (longituginal relaxation time) $T_1$ は**古典的**状態の寿命であり，通常 $T_2$ より長い．

### コラム 7.1: 方形井戸と q ビット

量子システムの 1 つの原型は「方形井戸」(square well) と呼ぶものである．これは 1 次元の箱の中の粒子であり，Schrödinger の方程式 (2.86) に従って振る舞う．このシステムの Hamiltonian は $H = p^2/2m + V(x)$ で与えられ，ここで $0 < x < L$ に対して $V(x) = 0$，それ以外は $V(x) = \infty$ である．位置基底で表現したエネルギー固有状態は：

$$|\psi_n\rangle = \sqrt{\frac{2}{L}}\sin\left(\frac{n\pi}{L}x\right), \tag{7.1}$$

ここで $n$ は整数, $|\psi_n\rangle = e^{-iE_nt}|\psi_n\rangle$, $E_n = n^2\pi^2/2mL^2$ である．これらの状態は離散的スペクトルを持つ．特に実験で 2 つの最低エネルギー準位だけを考える状況を想定する．興味の対象とする任意の波動関数を $|\psi\rangle = a|\psi_1\rangle + b|\psi_2\rangle$ と定義する．

$$|\psi(t)\rangle = e^{-i(E_1+E_2)t/2}[ae^{-i\omega t}|\psi_1\rangle + be^{i\omega t}|\psi_2\rangle], \tag{7.2}$$

ここで $\omega = (E_1 - E_2)/2$ であり，$a$ と $b$ のみに注目すればよくこの状態を**抽象的に**2 成分ベクトル $|\psi\rangle = \begin{bmatrix} a \\ b \end{bmatrix}$ と書く．この 2 準位システムは q ビットを表す！ 我々の 2 準位システムは q ビットのような変換をするであろうか？時間が経過するとこの q ビットは実効的 Hamiltonian $H = \hbar\omega Z$ の影響下で変化するが，これは回転フレームに移行すると無視できる．この q ビットに演算を行うには $H$ に摂動を与える．次の付加項を $V(x)$ に加える影響を考えよう：

$$\delta V(x) = -V_0(t)\frac{9\pi^2}{16L}\left(\frac{x}{L} - \frac{1}{2}\right). \tag{7.3}$$

想定する 2 準位システムの基底において行列要素 $V_{nm} = \langle\psi_n|\delta V(x)|\psi_m\rangle$,

$V_{11} = V_{22} = 0$, $V_{12} = V_{21} = V_0$ を用いて，$V_0$ の最低次で $H$ への摂動が $H_1 = V_0(t)X$ となるようにこの式を書き換える．これは $\hat{x}$ 軸の回りの回転を引き起こす．同様のテクニックを用いてポテンシャル関数を操作することにより，他の単一 q ビット演算を行うことができる．

これは単一 q ビットを方形井戸ポテンシャル中の 2 つの最低レベルで表現することができて，ポテンシャルの簡単な摂動が計算演算として q ビットに効果を及ぼす方法を示している．しかし同時に摂動は高次の効果をもたらす．実際の物理システムでは井戸は無限に深くなく，他の準位もモデル中に現れて 2 準位近似が綻び始める．また実際は制御システムももう 1 つの量子システムなので，量子計算をするシステムと結合する．これらの問題がコヒーレンス劣化につながる．

### 7.2.2　ユニタリー変換の性能

閉じた量子システムはその Hamiltonian で記述されるユニタリーな時間発展をするが，量子計算を行うには（4.5 節で述べたように）普遍的集まりから**任意に**選んだユニタリー変換を実行して，Hamiltonian を制御できなければならない．例えば，単一スピンは Hamiltonian $H = P_x(t)X + P_y(t)Y$ のもとで時間発展をする．ここで $P_{\{x,y\}}$ は古典的に制御できるパラメータである．演習 4.10 より $P_x$ と $P_y$ を適切に操作すると，単一スピンの回転が実行できることを知っている．

4.5 節の定理によれば，任意のユニタリー変換は単一スピン演算と制御 NOT ゲートで構成できるので，これら 2 種類の量子論理ゲートを実現することが量子計算実験の当然のゴールになる．しかし q ビットに個別にアドレスする能力や，これらのゲートを適用して q ビットや q ビット対を選び出す能力も暗に要求されている．多くの物理システムにとってこれを行うのは簡単でない．例えばイオントラップにおいて，多くのイオンの 1 つを選択的に励起するためにレーザ光を照射するが，イオンが空間的に 1 波長程度離れた場合にのみ選択が可能である．

ユニタリー変換において表に出ない欠陥がコヒーレンス劣化を引き起こすことがある．8 章（第 III 巻）で我々はランダムなキック（単一スピンに与える $\hat{z}$ 軸の回りの僅かな回転）によって，量子状態の相対位相で表される量子情報が失わ

れることを学ぶ．同様に系統的誤りが累積してそれを元に戻すに必要な情報が失われると，コヒーレンスが劣化する．さらに Hamiltonian 中の制御パラメータは近似的に古典的制御であるにすぎない．実際に制御システムはもう 1 つの量子システムであり，真の Hamiltonian ならば制御システムから量子コンピュータへの反作用を含まねばならないところである．例えば上の例で $P_x(t)$ の代わりに，実際には $P_x(t) = \sum_k \omega_k(t)(a_k + a_k^\dagger)$ かそれに似た量が共振器内の光子電界を表す Jaynes-Cummings 型の原子・光子相互作用 Hamiltonian （7.5.2 項）を含む．q ビットと相互作用をした後で光子が q ビット状態の情報を運び去ることが起こり得て，これがコヒーレンス劣化の過程となる．

最小の達成可能な忠実度 (fidelity) $\mathcal{F}$ （9 章：第 III 巻）と，単一スピンの回転や制御 NOT ゲートのような基本的演算を行うに必要な最大時間 $t_{op}$ の 2 つはユニタリー変換に対する重要な性能指数である．

### 7.2.3 信頼できる初期状態の作成

古典的場合も含めて便利に計算できるための最も重要な要求条件の 1 つは所望の入力が準備できることである．もし完全な計算ができる箱があったとしても数が入力できなければ何の役に立つだろうか？ 古典的機械では確定的入力状態を作り出すことにほとんど困難はない — 単に所望の構成にスイッチを入れるとそれが入力状態となっている．しかし，q ビットの実現法によっては量子システムにおいてこれが非常に困難なことがある．

ユニタリー変換で任意の他の入力状態に変えることができるので，1 つの特定の量子状態を高い忠実度で（繰り返し）作り出すことだけで十分である．例えば $n$ 個のスピンを状態 $|00\ldots0\rangle$ に置ければよい．熱的擾乱によりその状態に長く留まっていないかも知れないが，それは表現の選択の問題である．

入力状態の準備はたいていの物理システムにとって重要な問題である．例えば，イオンを基底状態まで物理的に冷却すると良い入力状態になるが（7.6 節），これは困難な問題である．さらに量子コンピュータのアンサンブルを含む物理システムにおいては別の問題が生じる．核磁気共鳴（7.7 節）では各分子が 1 つのコンピュータと考えてよく，測定可能な信号強度を得るには多数の分子が必要になる．q ビットは比較的長い時間任意の重ね合せ状態に留まっているが，状態 $|0\rangle$ と $|1\rangle$

の間のエネルギー差 $\hbar\omega$ が $k_{\rm B}T$ よりもはるかに小さいので，全分子の q ビットをすべて同じ状態に置くのは難しい．他方で単にシステムを平衡状態に置くと，密度行列 $\rho \approx e^{-\mathcal{H}/k_{\rm B}T}/\mathcal{Z}$ を持つよく知られた熱平衡状態が実現できる．ここで $\mathcal{Z}$ は $\mathrm{tr}(\rho) = 1$ を維持するための正規化係数である．

入力状態の準備に関して 2 つの性能指数があげられる： 与えられた状態 $\rho_{in}$ に作り得る初期状態の最小の忠実度と，$\rho_{in}$ のエントロピーである．エントロピーが重要である理由は，例えば $\rho_{in} = I/2^n$ を高い忠実度で準備するのは非常に容易であるが，これはユニタリー変換で不変なので量子計算に使えない！ 理想的には入力状態はエントロピー 0 の純粋状態であることが望ましい．一般に入力状態のエントロピーが 0 でないと出力結果から答を取り出しにくくなる．

### 7.2.4　出力結果の測定

量子コンピュータにはどんな測定能力が必要か？ ここでの議論で測定とは，1 個またはそれ以上の q ビットと古典システムを結合させる過程である．その過程においてある時間間隔後に q ビット状態が古典システムの状態により表される．例えば，2 準位原子の基底状態と励起状態で表される q ビット状態 $a|0\rangle + b|1\rangle$ は，励起状態にポンピングして蛍光を見れば測定できる．もし光電子増倍管によって蛍光が検出されたことを電位計が示したならば q ビットは $|1\rangle$ 状態に収縮し，この現象は確率 $|b|^2$ で起きる．そうでなければ電位計は電荷を検出せず q ビットは状態 $|0\rangle$ に収縮する．

量子計算の測定過程における重要な性質は波動関数の収縮であり，これが射影測定を行ったときに何が起きるかを記述する（2.2.5 項：第 I 巻）．良い量子アルゴリズムの出力は，測定されたときに役に立つ答を高い確率で与える重ね合せ状態である．例えば，Shor の素因数分解アルゴリズムのあるステップは，測定結果から $qc/r$ に近い整数 $r$ を見出すことである．ここで $q$ は Hilbert 空間の次元である．出力状態は実際にすべての可能な値 $c$ の一様な重ね合せに近いが，測定によりこれが単一のランダムな整数に収縮して，（5 章で述べた連分数展開を用いて）$r$ が高い確率で決定される．

測定に伴い多くの困難が予想される．例えば，効率の悪い検出器や増幅器の熱雑音があると，上述の方式で測定される q ビットから得られる情報が減少する．

さらに射影測定（これは時に「強い測定」とも呼ばれる）は実行が難しいことが多い．これを行うには量子システムと古典的システムの結合が大きくて，スイッチできる必要がある．希望しないときに測定が行われてはならない．そうでなければ測定によってコヒーレンスが劣化する．

しかし驚くべきことに強い測定は必要でない．スイッチを切らずに連続的に実行する弱い測定が量子計算には有用である．これが可能になるのは測定の結合に比べて短時間で計算が終了し，かつ多くの量子コンピュータのアンサンブルを使うときである．これらのアンサンブルは全体として巨視的観測が可能で量子状態を示す信号を与える．アンサンブルを使うと別の問題が生じる．例えば，素因数分解のアルゴリズムにおいて測定出力が $q\langle c\rangle/r$ ならば，$c$ の平均値である $\langle c\rangle$ は必ずしも整数でないので（つまり連分数展開ができないので）アルゴリズムが失敗する．幸いアンサンブル平均の読み出しで働くように，量子アルゴリズムを修正することができる．これについては 7.7 節でさらに議論する．

測定能力に関する良い性能指数は信号対雑音比（SNR）である．これは測定装置を量子システムに結合したときに得られる固有の信号強度であると共に，測定の非効率さの原因を説明する．

## 7.3 調和振動子による量子コンピュータ

実現可能な量子コンピュータに対する完全な物理モデルについて続ける前に，一休みして非常に基本的システム — 単純調和振動子— について考え，なぜこれが良い量子コンピュータにならないかを議論しよう．この例で用いる定式化は他の物理システムを研究する基礎として役に立つ．

### 7.3.1 物理的装置

単純調和振動子の例は放物線ポテンシャル $V(x) = m\omega^2x^2/2$ 中の粒子である．例えば，これは古典的世界でバネにつながった質量であり，エネルギーがバネのポテンシャルエネルギーと質量の運動エネルギーの間で行き来するのに応じて，往復の振動をする．別の例は共振電気回路であり，インダクタとキャパシタの間をエネルギーが行き来する．これらの場合，システムの全エネルギーは連続パラ

メータである．

外界との結合が非常に小さい量子領域では，システムの全エネルギーは離散的値だけをとる．例えば高い $Q$ の共振器に閉じ込められた単一モードの電磁放射が良い例であり，エネルギーの全量は（固定したずれを除いて）基本的定数 $\hbar$ と閉じ込められた放射の周波数 $\omega$ で決まるエネルギー尺度 $\hbar\omega$ の整数倍のみをとる．

単純調和振動子の離散的エネルギー固有状態の集合に $|n\rangle$ というラベルを付ける．ここで $n = 0,\ 1, \ldots, \infty$ である．これら状態の有限な部分集合を取り出して q ビットを表すことにより量子計算と関連付けることができる．これらの q ビットは共振器の性能指数 $Q$ のような物理パラメータで決まる寿命を持っており，共振器壁の反射率を増すと大きくできる．さらにシステムを時間発展させて，ユニタリー変換を適用することができる．しかし以下で明らかになるがこの方式には問題がある．最初システムの Hamiltonian を調べることから始めて，制御 NOT のような簡単な量子ゲートを実現する方法を議論しよう．

## 7.3.2　Hamiltonian

1 次元放物線ポテンシャル中の粒子に対する Hamiltonian は

$$H = \frac{p^2}{2m} + \frac{1}{2}m\omega^2 x^2, \tag{7.4}$$

ここで $p$ は粒子の運動量オペレータ，$m$ は質量，$x$ は位置オペレータ，$\omega$ はポテンシャルの深さに関係するパラメータである．$x$ と $p$ がこの表現のオペレータであることに留意して（コラム 7.2 参照）これを書き換えると：

$$H = \hbar\omega\left(a^\dagger a + \frac{1}{2}\right), \tag{7.5}$$

ここで $a^\dagger$ と $a$ は次式で定義される生成オペレータ (creation operator)，消滅オペレータ (annihilation operator) である：

$$a = \frac{1}{\sqrt{2m\hbar\omega}}\left(m\omega x + ip\right) \tag{7.6}$$

$$a^\dagger = \frac{1}{\sqrt{2m\hbar\omega}}\left(m\omega x - ip\right). \tag{7.7}$$

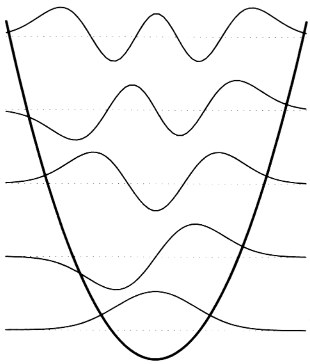
零点エネルギー $\hbar\omega/2$ は観測されない全体の位相因子に寄与するだけであり，ここでの目的には無視できる．

## コラム 7.2: 量子調和振動子

実世界を量子的に記述する際に調和振動子は非常に重要で便利な概念であり，その性質を理解する最初の良い方法は，Hamiltonian (7.4) のエネルギー固有状態を決定することである．これを簡単に行う方法は，$x = \pm\infty$ で $\psi(x) \to 0$ および $\int |\psi(x)|^2 dx = 1$ の条件下で Schrödinger 方程式を解いて，$\psi(x)$ とエネルギー固有状態 $E$ を求めることである．

$$\frac{\hbar^2}{2m}\frac{d^2\psi_n(x)}{dx^2} + \frac{1}{2}m\omega^2 x^2 \psi_n(x) = E\psi_n(x). \tag{7.8}$$

最初の 5 つの解を略図で示す：




これらの波動関数は調和振動子の粒子がポテンシャル内の異なる位置で見出される確率振幅を記述する．

この図は物理システムが座標空間で何をしているかを直観的に示すかも知れないが，我々が一般的に興味を持つのは状態の抽象的な**代数的**性質である．具体的には $|\psi\rangle$ がエネルギー $E$ を持つ式 (7.8) を満たすとする．式 (7.6), (7.7) のように $a$ と $a^\dagger$ を定義すると，$[H, a^\dagger] = \hbar\omega a^\dagger$ なので

$$Ha^\dagger|\psi\rangle = \left([H, a^\dagger] + a^\dagger H\right)|\psi\rangle = (\hbar\omega + E)a^\dagger|\psi\rangle, \tag{7.9}$$

つまり，$a^\dagger|\psi\rangle$ はエネルギー $E + \hbar\omega$ を有する $H$ の固有状態である！ 同様に

$a|\psi\rangle$ はエネルギー $E - \hbar\omega$ を有する固有状態である．こういう理由で $a^\dagger$ と $a$ をそれぞれ上昇オペレータ (raising operator)，下降オペレータ (lowering operator) とも呼ぶ．さらに任意の $n$ に対して $a^{\dagger n}|\psi\rangle$ はエネルギー $E + n\hbar\omega$ を有する固有状態である．こうして無限の数のエネルギー固有状態が存在し，そのエネルギーは $\hbar\omega$ の等間隔で分布する．さらに $H$ は正の定符号なので $a|\psi_0\rangle = 0$ なる $|\psi_0\rangle$ が存在し，これが最低エネルギーを持つ $H$ の固有状態 — 基底状態 (ground state) — である．これらの結果により量子調和振動子の基礎が効率良く把握できて，この状態に対して簡潔な記号 $|n\rangle$ を用いることができる．ここで $n$ は整数で，$H|n\rangle = \hbar\omega(n + 1/2)|n\rangle$ である．調和振動子は多くの異なる物理システムの形をとって現れるので，本章では $|n\rangle$, $a$, $a^\dagger$ をしばしば用いる．

$H$ の固有状態 $|n\rangle$ は次の性質を持っている．

$$a^\dagger a|n\rangle = n\,|n\rangle \tag{7.10}$$

$$a^\dagger|n\rangle = \sqrt{n+1}\,|n+1\rangle \tag{7.11}$$

$$a|n\rangle = \sqrt{n}\,|n-1\rangle. \tag{7.12}$$

ここで $n = 0,\ 1, \ldots$ である．単純調和振動子との相互作用を表すには $a$ と $a^\dagger$ を含む付加項を導入して，振動子間の相互作用に $a_1{}^\dagger a_2 + a_1 a_2{}^\dagger$ のような項を導入すると便利であることが後でわかる．しかし当面単一の振動子に話を限る．

**演習 7.1:** $x$ と $p$ が可換でなく，実際には $[x,p] = i\hbar$ であることを使って，$a^\dagger a = H/\hbar\omega - 1/2$ を明示的に示せ．

**演習 7.2:** $[x,p] = i\hbar$ が与えられたとき，$[a, a^\dagger]$ を計算せよ．

**演習 7.3:** $[H,a]$ を計算し，その結果を使ってもし $|\psi\rangle$ がエネルギー $E \geq n\hbar\omega$ を有する $H$ の固有状態ならば，$a^n|\psi\rangle$ はエネルギー $E - n\hbar\omega$ を有する固有状態であることを示せ．

**演習 7.4:** $|n\rangle = \dfrac{(a^\dagger)^n}{n!}|0\rangle$ を示せ．

**演習 7.5:** 式 (7.11) と式 (7.12) は式 (7.10) および正規化条件 $\langle n|n\rangle = 1$ と矛盾しないことを示せ．

固有状態の時間発展は Schrödinger の方程式 (2.86)（第 I 巻）を解くと得られる．これより状態 $|\psi(0)\rangle = \sum_n c_n(0)|n\rangle$ は次のような時間発展をする：

$$|\psi(t)\rangle = e^{-iHt/\hbar}|\psi(0)\rangle = \sum_n c_n e^{-in\omega t}|n\rangle. \tag{7.13}$$

今後の議論のために，任意の状態を完全に準備することができて，システム状態を射影測定をすることができるとする（2.2.3 項：第 I 巻）．それ以外の場合には外界との相互作用がなくて，システムが完全に閉じていると仮定する．

### 7.3.3　量子計算

上で述べた単一の単純調和振動子を使って量子計算をしたいとする．どうすればよいか？ 最も自然な q ビット表現の選択はエネルギー固有状態 $|n\rangle$ である．このように選択すると制御 NOT を次のように実行できる．この変換は 2 個の q ビット状態に次の写像を実行することを思い出そう：

$$\begin{aligned} |00\rangle_L &\to |00\rangle_L & |01\rangle_L &\to |01\rangle_L \\ |10\rangle_L &\to |11\rangle_L & |11\rangle_L &\to |10\rangle_L, \end{aligned} \tag{7.14}$$

（ここで添字 $L$ は調和振動子の基底状態ではなく，「論理」状態であることを明らかに区別するために使っている．）これら 2 個の q ビットを次の写像を使って符号化する：

$$\begin{aligned} |00\rangle_L &= |0\rangle & |01\rangle_L &= |2\rangle \\ |10\rangle_L &= (|4\rangle + |1\rangle)/\sqrt{2} & |11\rangle_L &= (|4\rangle - |1\rangle)/\sqrt{2}. \end{aligned} \tag{7.15}$$

次に $t = 0$ においてこれら基底状態 (basis state) が張る状態からシステムが出発し，単純に時間 $t = \pi/\omega$ までシステムが発展するとする．これによりエネルギー固有状態が $|n\rangle \to \exp(-i\pi a^\dagger a)|n\rangle = (-1)^n|n\rangle$ に変換して，$|0\rangle, |2\rangle, |4\rangle$ は変化しないが $|1\rangle \to -|1\rangle$ となる．この結果所望の制御 NOT ゲート変換が得られる．

一般に物理システムがユニタリー変換を実行できる必要十分条件は，Hamiltonian $H$ で定義されたシステムの時間発展オペレータ $T = \exp(-iHt)$ が，単に $U$ とほとんど同じ固有値スペクトルを有することである．上の例では固有値が $+1$ と $-1$ だけなので制御 NOT ゲートを実行するのは容易であった．調和振動子に対する時間発展オペレータから同じ固有値が得られるように，符号化を調整することが容易にできた．振動子に対する Hamiltonian はほとんどどんな固有値スペクトルであっても実現できるように摂動を加えることができて，このシステムの無限の固有状態に写像するだけで幾つの q ビットでも表現することができる．これはもしかすると 1 つの単純調和振動子の中にすべての量子コンピュータが実現できるかも知れないことを示唆している！

### 7.3.4　欠　点

もちろん上の筋書きには問題が多い．基本ゲートからオペレータを構築する方法を知っていても，ある量子計算に対するユニタリーオペレータの固有値スペクトルをいつも知っているわけでないのは明らかである．量子アルゴリズムが目指す多くの問題に対して，固有値スペクトルに関する知識は解に関する知識と実際上同等である！

もう 1 つ明らかに問題なのは，2 つのユニタリー変換を縦続すると一般に互いに関連しない固有値を持つ新しい変換になるので，上で用いたテクニックでは縦続した計算ができないことである．

最後に単一の調和振動子を用いて量子計算を行うという考えは，情報のディジタル表現の原理を無視しているので成り立たない．$2^n$ 次元の Hilbert 空間を単一の調和振動子の状態空間に写像すると，エネルギー $2^n\hbar\omega$ の状態ができることになる．これに対して同じ Hilbert 空間はたかだか $n\hbar\omega$ のエネルギーを有する $n$ 個の 2 準位量子システムでも得られる．$2^n$ 個の設定値を持つ古典的ダイヤルと古典的 $n$ ビットのレジスタの間を比較するのと同じである．量子計算は**ディジタル**計算に基づいており，アナログ計算ではない．

調和振動子量子コンピュータの主要な特徴を下にまとめる．（我々が考えるそれぞれのシステムも，同じように対応する節の最後にまとめを述べる．）これで単一振動子を終えて，次に光子や原子でできた調和振動子のシステムに進む．

**調和振動子量子コンピュータ**

- **q ビット表現：** 単一の量子振動子のエネルギー準位 $|0\rangle,\ |1\rangle,\ \ldots,|2^n\rangle$ で $n$ 個の q ビットができる．
- **ユニタリー時間発展：** 固有値スペクトルを Hamiltonian $H = a^\dagger a$ と一致させると，任意の変換 $U$ が実現できる．
- **初期状態の準備：** 考慮せず．
- **読み出し：** 考慮せず．
- **欠点：** ディジタル表現でない！ また任意の $U$ の固有値は一般に未知なので，それに対する変換を実現するために固有値を一致させることができない．

## 7.4 光子による量子コンピュータ

光子は量子ビットを表現するための魅力ある物理システムである．光子には電荷がなく，光子同士やたいていの物質との相互作用も強くない．低損失光ファイバで光子を長距離にわたって導いたり，位相シフタで効率良く遅延させたり，ビームスプリッタで容易に重ね合わせたりすることができる．光子は 2 重スリット実験で作られる干渉のような特徴的量子現象を示す．さらに原理上は相互作用を仲介する非線形光学媒質を使って，光子を互いに相互作用させることができる．これらは理想的筋書きであり，実現するには多数の解決すべき問題があるが，部品や構成や光子情報処理装置の欠点を調べることによって多くのことが学べる．本節ではこれらのことを見ていく．

### 7.4.1 物理的装置

まず単一光子とは何か，その量子状態を如何に表現できるか，またその光子を取り扱う便利な実験装置とは何かについて考えることから始める．位相シフタ，ビームスプリッタ，非線形 Kerr 媒質の古典的振る舞いについても述べる．

光子は次のようにして q ビットを表現することができる．単純調和振動子の議論で見たように，電磁界共振器は単位 $\hbar\omega$ で量子化される．その各々の量子を光子と呼ぶ．共振器はゼロと 1 つの光子の重ね合せを含むことができ，この状態を q ビット $c_0|0\rangle + c_1|1\rangle$ で表すことができる．しかし少し異なる方法もある．全エ

ネルギーが $\hbar\omega$ である 2 つの共振器を考え，光子が一方の共振器にあるか（$|01\rangle$）あるいは他方にあるか（$|10\rangle$）が q ビットの 2 つの状態であると考える．したがって重ね合せの物理的状態は $c_0|01\rangle + c_1|10\rangle$ と書くことができて，これを **2 重軌道表現**(dual rail representation) と呼ぶ．我々は共振器中でなく，自由空間を波束として進行する単一光子に注目して，これに波束に沿って動く共振器が付随すると想像することができる．このようにして我々の q ビット状態にある各共振器を異なる空間モードに対応させることができる．

実験室で単一光子を発生する 1 つの方法は，レーザ出力を減衰させることである．レーザ光は次式で定義されるコヒーレント状態と呼ぶ状態をとる：

$$|\alpha\rangle = e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} \; |n\rangle, \tag{7.16}$$

ここで $|n\rangle$ は $n$ 個の光子を有するエネルギー固有状態である．この状態はこれまで量子光学分野の研究テーマであり，ここでは述べないが多くの素晴らしい性質を持っている．コヒーレント状態はレーザしきい値より高くポンプされたレーザのように，駆動された発振器から自然に放出されることを理解していれば，ここでは十分である．平均エネルギーは $\langle\alpha|n|\alpha\rangle = |\alpha|^2$ である．減衰するとコヒーレント状態は弱いコヒーレント状態になるだけであり，弱いコヒーレント状態は高い確率で 1 個の光子だけを持つようにできる．

**演習 7.6:（光子消滅の固有状態）**　コヒーレント状態は光子消滅オペレータの固有状態であることを証明せよ，つまりある定数 $\lambda$ に対して $a|\alpha\rangle = \lambda|\alpha\rangle$ を示せ．

例えば $\alpha = \sqrt{0.1}$ に対して我々が得る状態は $\sqrt{0.90}|0\rangle + \sqrt{0.09}|1\rangle + \sqrt{0.002}|2\rangle + \cdots$ である．したがって，もし光が減衰器を通った後でこうなれば，95%以上の確率で単一光子であり，失敗確率は 5%以下となる．90%以上の時間は全く光子が到来せず，この光源は単位時間に 0.1 個の割合で光子を出す．この光源が何時光子を出したのか出さなかったのかを（何か古典的な読み出し方で）知ることができないし，この種の光源を 2 つ同期させることもできない．

パラメトリック下方変換を使うと 2 つの光子に同期性を与えることができる．$KH_2PO_4$ のような非線形光学媒質に周波数 $\omega_0$ の光子を送り込み，周波数 $\omega_1 + \omega_2 =$

$\omega_0$ の光子対を発生する．このとき $\vec{k}_1 + \vec{k}_2 = \vec{k}_0$ となるように運動量も保存される．単一光子 $\omega_2$ が（破壊的に）検出されると，単一光子 $\omega_1$ が存在することがわかる（図 7.2）．（2 光子やそれ以上でなく）単一光子が検出されたときにのみ開くゲートにこれを結合して，多数の下方変換光源の出力に適当な遅延を加えると，原理上検出器とゲートの解像時間内で時間的に同期して伝搬する複数の単一光子を得ることができる．

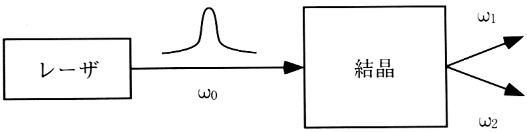



**図 7.2:** 単一光子を発生するためのパラメトリック下方変換法

いろいろな技術を使って単一光子は，広い波長帯にわたって高い量子効率で検出できる．我々の目的に最も重要な検出器の特性は，特定の空間モード内において 0 か 1 の光子を高い確率で決定する能力である．これは結果として 2 重軌道表現に対して計算基底における射影測定になる．実際に不完全性があれば単一光子を検出する確率が低下する．光検出器の**量子効率** $\eta$（$0 \geq \eta \geq 1$）は検出器に入射する単一光子が，検出器電流に貢献する光キャリア対を発生する確率である．検出器のその他の重要な特性には帯域幅（時間応答），雑音，および光子が入射しなくても光キャリアができてしまう「暗計数」(dark count) がある．

光子状態を操作するために実験的に作り易いデバイスを 3 つあげると，反射鏡，位相シフタ，ビームスプリッタがある．高反射率の反射鏡は光子を反射してその空間中の伝搬方向を変える．損失 0.01% の反射鏡も稀ではなく，我々のシナリオではこれを当然のこととして取り扱う．位相シフタは透明媒質の平板に他ならず，その屈折率 $n$ が自由空間屈折率 $n_0$ と異なる．例えば，通常の硼珪酸ガラスでは光学波長において $n \approx 1.5\, n_0$ である．そのような媒質中を長さ $L$ だけ伝搬すると光子の位相は $e^{ikL}$ だけ変化する．ここで $k = n\omega/c_0$，$c_0$ は真空中の光速である．したがって，位相シフタを通る光子は自由空間中を同じ距離伝搬する光子に比べて $e^{i(n-n_0)L\omega/c_0}$ だけ大きい位相シフトを生じる．

もう 1 つの便利な部品はビームスプリッタであり，これは不十分に金属蒸着されたガラス板にすぎない．入射光の一部 $R$ を反射して $1 - R$ を透過する．実験室で

は図 7.3 に模式的に示すようにビームスプリッタは 2 つのプリズムで作られ，金属層が 2 つプリズムの間にはさまれている．ビームスプリッタの**角度** $\theta$ を $\cos\theta = R$ で定義すると便利である．この角度は部分的反射率の量をパラメータとするものであって，ビームスプリッタの物理的な向きとは関係がない．このデバイスの 2 入力と 2 出力の関係は：

$$a_{out} = a_{in}\cos\theta + b_{in}\sin\theta \tag{7.17}$$

$$b_{out} = -a_{in}\sin\theta + b_{in}\cos\theta, \tag{7.18}$$

ここで古典的に $a$ と $b$ は 2 つのポートの放射の電磁界と考えてよい．この定義では我々の目的のために標準的でない位相の使い方をしていることに注意する．特に 50/50 のビームスプリッタでは $\theta = 45°$ である．

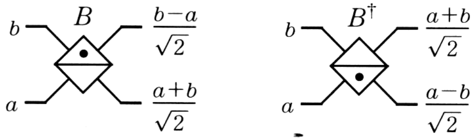



**図 7.3:** 光ビームスプリッタの模式図．2 つの入力ポート，2 つの出力ポート，および 50/50 ビームスプリッタ（$\theta = \pi/4$）に対する位相関係を示す．右のビームスプリッタは左を逆転したものである（内部に書かれた点で両者を区別する）．モードオペレータ $a, b$ に対する入出力関係は $\theta = \pi/4$ に対応する．

最後に示す便利な部品は非線形光学により作られる．この材料はそれを通る光の全強度 $I$ によって屈折率 $n$ が変化する：

$$n(I) = n + n_2 I. \tag{7.19}$$

この効果を光 Kerr 効果と呼び，ガラスや砂糖水のようなありふれた材料で（非常に弱く）起きる．不純物を添加したガラスで $n_2$ は $10^{-14} \sim 10^{-7}\mathrm{cm}^2/\mathrm{W}$，半導体で $10^{-10} \sim 10^2$ の値をとる．実験的に生じる現象では等強度の 2 つのビームが Kerr 媒質中を共に伝搬すると，各ビームは単独で伝搬した場合に比べて付加的な位相シフト $e^{in_2IL\omega/c_0}$ を受ける．これは長さ $L$ が任意に長い理想的な場合であって，残念ながらたいていの Kerr 媒質では吸収があったり所望の空間モードから散乱が生じるので，このように動作しないことが多い．7.4.3 項で議論するが，これが単一光子の量子コンピュータが実際的でない主たる理由である．

次にこれら光部品を量子的に記述する．

### 7.4.2 量子計算

位相シフタ，ビームスプリッタおよび非線形の光 Kerr 媒質を使って，2 重軌道表現の $c_0|01\rangle + c_1|10\rangle$ で表した単一光子で符号化された量子情報に，任意のユニタリー変換を適用することができる．各デバイスを量子力学的 Hamiltonian 表示で記述すると，これがどのように働くかは次のように理解できる．

電磁放射の共振器モードの時間発展は 7.3.2 項で見たように量子力学的に調和振動子でモデル化できる．$|0\rangle$ は真空状態，$|1\rangle = a^\dagger|0\rangle$ は単一光子状態，そして一般に $|n\rangle = \frac{a^{\dagger n}}{\sqrt{n!}}|0\rangle$ は $n$ 光子数状態である．ここで $a^\dagger$ はモードの生成オペレータである．自由空間の時間発展は次の Hamiltonian で記述される：

$$H = \hbar\omega a^\dagger a. \tag{7.20}$$

式 (7.13) を適用すると状態 $|\psi\rangle = c_0|0\rangle + c_1|1\rangle$ は発展して，$|\psi(t)\rangle = c_0|0\rangle + c_1 e^{-i\omega t}|1\rangle$ となることがわかる．2 重軌道表現では，自由な時間経過により $|\varphi\rangle = c_0|01\rangle + c_1|10\rangle$ の全体位相だけが変化し，これは検出されないので便利である．したがって，この多重状態に対して時間発展 Hamiltonian はゼロである．

**位相シフタ**　位相シフタ $P$ は通常の時間発展と同様の働きをするがその割合が異なり，それを通過するモードにだけ局在化されて働く．これは大きな屈折率を持つ媒質中で光が減速することによる．具体的に屈折率 $n$ の媒質中を距離 $L$ だけ進むには $\Delta/\omega \equiv (n - n_0)L/c_0$ だけ余計に時間がかかる．例えば，真空状態に対して $P$ は何もせず $P|0\rangle = |0\rangle$，単一光子状態に対しては $P|1\rangle = e^{i\Delta}|1\rangle$ となる．

$P$ によって 2 重軌道状態に対して便利な論理演算ができる．1 つのモードに対して位相シフタを置くと同じ距離を伝搬するが，位相シフタを通らない他のモードに比べてそのモードの位相変化が遅れる．無関係な全体の位相を除いて，この変換で 2 重軌道状態は $c_0|01\rangle + c_1|10\rangle$ から $c_0 e^{-i\Delta/2}|01\rangle + c_1 e^{i\Delta/2}|10\rangle$ に変化する．4.2 節よりこの変換は回転：

$$R_z(\Delta) = e^{-iZ\Delta/2} \tag{7.21}$$

に他ならない．ここで論理的な 0 を $|0_L\rangle = |01\rangle$, 1 を $|1_L\rangle = |10\rangle$ と表し，$Z$ は通常の Pauli のオペレータである．したがって，$P = \exp(-iHL/c_0)$ は Hamiltonian：

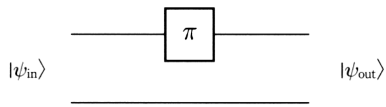
$$H = (n_0 - n)Z \tag{7.22}$$

のもとでの時間は発展により生じると考えてよい．

**演習 7.7:** 次図の回路において上の配線が $|01\rangle$ モード，下の配線が $|10\rangle$ モードに対応し，箱の中の $\pi$ が位相変化 $\pi$ を表すならば，この回路は 2 重軌道状態を

$$|\psi_{out}\rangle = \begin{bmatrix} e^{i\pi} & 0 \\ 0 & 1 \end{bmatrix} |\psi_{in}\rangle \tag{7.23}$$

により変換することを示せ．




この「光回路」において自由空間中の伝搬は位相変化を表すために上のような集中回路素子で表示されることに注意する．2 重軌道表現において時間発展 (7.20) は，観測できないグローバル位相だけ論理状態を変化させるだけなので無視することができて，相対的位相だけを考えればよい．

**演習 7.8:** $|\alpha\rangle$ をコヒーレント状態として，$P|\alpha\rangle = |\alpha e^{i\Delta}\rangle$ を示せ．（一般に $\alpha$ は複素数であることに注意.）

**ビームスプリッタ**　同様の Hamiltonian による記述がビームスプリッタに対して可能であるが，それを現象的に述べる代わりに，Hamiltonian から始めて，期待される式 (7.17), (7.18) の古典的振る舞いがそこから生じることを示す．ビームスプリッタは 2 モードに働くことを思い出し，生成（消滅）オペレータ $a$ ($a^\dagger$), $b$ ($b^\dagger$) で記述する．Hamiltonian は：

$$H_{bs} = i\theta(ab^\dagger - a^\dagger b). \tag{7.24}$$

ビームスプリッタは次のユニタリー変換を実行する：

$$B = \exp[\theta(a^\dagger b - ab^\dagger)]. \tag{7.25}$$

変換 $B$ を $a$ と $b$ に実行したものは次のように求められ，これは後で便利になる：

$$BaB^\dagger = a\cos\theta + b\sin\theta \quad \text{および} \quad BbB^\dagger = -a\sin\theta + b\cos\theta. \tag{7.26}$$

これらの関係を次の Baker-Campbell-Hausdorf の公式（演習 4.49 参照）を使って証明する：

$$e^{\lambda G} A e^{-\lambda G} = \sum_{n=0}^{\infty} \frac{\lambda^n}{n!} C_n, \tag{7.27}$$

ここで $\lambda$ は複素数，$A$, $G$ および $C_n$ はオペレータ，$C_n$ は交換子の漸化式 $C_0 = A$, $C_1 = [G,\ C_0]$, $C_2 = [G,\ C_1]$, $C_3 = [G,\ C_2], \ldots, C_n = [G,\ C_{n-1}]$ で定義される．$[a,\ a^\dagger] = 1$ と $[b,\ b^\dagger] = 1$ から，$G \equiv ab^\dagger - a^\dagger b$ に対して $[G, a] = b$ および $[G, b] = -a$ なので，$BaB^\dagger$ の展開における一連の係数は $C_0 = a$, $C_1 = [G,\ a] = b$, $C_2 = [G,\ C_1] = -a$, $C_3 = [G,\ C_2] = -[G,\ C_0] = -b$，一般に

$$C_{n\ \text{even}} = i^n a \tag{7.28}$$

$$C_{n\ \text{odd}} = -i^{n+1} b. \tag{7.29}$$

これより所望の結果が直接導ける：

$$\begin{aligned} BaB^\dagger &= e^{\theta G} a e^{-\theta G} && (7.30)\\ &= \sum_{n=0}^{\infty} \frac{\theta^n}{n!} C_n && (7.31)\\ &= \sum_{n\ \text{even}} \frac{(i\theta)^n}{n!} a - i \sum_{n\ \text{odd}} \frac{(i\theta)^n}{n!} b && (7.32)\\ &= a\cos\theta + b\sin\theta. && (7.33) \end{aligned}$$

変換 $BbB^\dagger$ は上式で $a$ と $b$ を入れ換えると容易に得られる．コラム 7.3 で説明するように，ビームスプリッタのオペレータはビームスプリッタと $SU(2)$ の代数の深い関係から生じていることに注意する．

量子論理ゲートの表現によれば，$B$ の演算を便利に実行できる．まず $B|00\rangle = |00\rangle$，つまり光子がいずれの入力モードにも入ってこなければいずれの出力モードからも出て行かない．モード $a$ に 1 個の光子が存在すると $|1\rangle = a^\dagger|0\rangle$ であることを思い出して

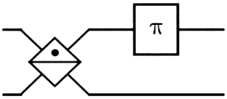
$$\begin{aligned} B|01\rangle &= Ba^\dagger|00\rangle = Ba^\dagger B^\dagger B|00\rangle = (a^\dagger\cos\theta + b^\dagger\sin\theta)|00\rangle \\ &= \cos\theta|01\rangle + \sin\theta|10\rangle. \end{aligned} \tag{7.34}$$

同様に $B|10\rangle = \cos\theta|10\rangle - \sin\theta|01\rangle$．したがって $|0_L\rangle$ と $|1_L\rangle$ の多重状態に対して $B$ は次のように書ける：

$$B = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} = e^{i\theta Y}. \tag{7.35}$$

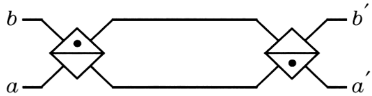
位相シフタとビームスプリッタを組み合わせると，任意の単一 q ビット演算を光子 q ビットに実行させることができる．これは定理 4.1 の結果であり，すべての単一 q ビット演算が $\hat{z}$-軸の回りの回転 $R_z(\alpha) = \exp(-i\alpha Z/2)$ と，$\hat{y}$-軸の回りの回転 $R_y(\alpha) = \exp(-i\alpha Y/2)$ から作ることができることを表している．位相シフタは $R_z$ 回転を実行し，ビームスプリッタは $R_y$ 回転を実行する．

**演習 7.9:（光 Hadamard ゲート）** 図に示す回路が 2 重軌道表現で表された単一光子状態に対して Hadamard ゲートとして働くこと，つまり全体の位相を除いて $|01\rangle \to (|01\rangle + |10\rangle)/\sqrt{2}$ および $|10\rangle \to (|01\rangle - |10\rangle)/\sqrt{2}$ であることを示せ．

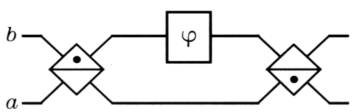



**演習 7.10:（Mach-Zehnder 干渉計）** 干渉計は 2 つのビームスプリッタで構成され，小さな位相シフトを測定するのに用いる光デバイスである．その基本原理がこの演習から理解できる．

(1) 次の回路は恒等 (identity) 演算を行うことに留意する．




(2) 次の回路が実行する（2 重軌道状態への）回転演算を $\varphi$ の関数として求めよ．



**演習 7.11:** $\theta = \pi/4$ に対する $B|2,0\rangle$ とは何か？

**演習 7.12:（古典的入力を有する量子ビームスプリッタ）** $|\alpha\rangle$ と $|\beta\rangle$ は式 (7.16) と同様に 2 つのコヒーレント状態とする．$B|\alpha\rangle|\beta\rangle$ は何か？（ヒント：$|n\rangle = \frac{(a^\dagger)^n}{\sqrt{n!}}|0\rangle$ を思い出そう．）

**コラム 7.3: $SU(2)$ 対称性と量子ビームスプリッタ**

Lie 群 $SU(2)$ と 2 つの結合調和振動子の代数の間には興味深い関係があり，量子ビームスプリッタ変換を理解するのに便利である．次式を確認する：

$$a^\dagger a - b^\dagger b \to Z \tag{7.36}$$

$$a^\dagger b \to \sigma_+ \tag{7.37}$$

$$ab^\dagger \to \sigma_-, \tag{7.38}$$

ここで $Z$ は Pauli のオペレータ，$\sigma_\pm = (X \pm iY)/2$ は Pauli の $X$ と $Y$ で定義した上昇，下降オペレータである．$a$, $a^\dagger$, $b$, $b^\dagger$ に対する交換関係から，これらの定義が Pauli のオペレータに対する通常の交換関係 (2.40) を満たすことが容易に証明できる．全光子数オペレータ $a^\dagger a + b^\dagger b$ は当然ながら $\sigma_z$, $\sigma_+$, $\sigma_-$ と可換であり，$SU(2)$ 空間での回転に対して不変である．通常の $SU(2)$ 回転オペレータ

$$R(\hat{n}, \theta) = e^{-i\theta\vec{\sigma}\cdot\hat{n}/2} \tag{7.39}$$

において $X = a^\dagger b + ab^\dagger$ と $Y = -i(a^\dagger b - ab^\dagger)$ を用い，$\hat{n}$ を $-\hat{y}$ 軸とすると求めるビームスプリッタのオペレータが得られる．

**非線形 Kerr 媒質**　Kerr 媒質の最も重要な効果は，2 つの光モード間に**相互位相変調**(cross phase modulation) を起こさせることである．これは Kerr 媒質中の原子により仲介された，光子間の相互作用を表す式 (7.19) の $n_2$ 項で古典的に記述される．この効果は次の Hamiltonian で量子力学的に記述される：

$$H_{xpm} = -\chi a^\dagger a b^\dagger b, \tag{7.40}$$

ここで $a$ と $b$ は媒質を通る 2 つのモードを表し，長さ $L$ の媒質に対して次のユニタリー変換を得る：

$$K = e^{i\chi L a^\dagger a b^\dagger b}. \tag{7.41}$$

$\chi$ は $n_2$ に関連した係数であり，通常 3 次の非線形感受率 $\chi^{(3)}$ と表記される．この Hamiltonian から期待される古典的振る舞いを導くことは，演習として読者に委ねる．

Kerr 媒質とビームスプリッタを組み合わせると，次のように制御 NOT ゲートが構成できる．単一光子状態に対して

$$K|00\rangle = |00\rangle \tag{7.42}$$

$$K|01\rangle = |01\rangle \tag{7.43}$$

$$K|10\rangle = |10\rangle \tag{7.44}$$

$$K|11\rangle = e^{i\chi L}|11\rangle, \tag{7.45}$$

$K|11\rangle = -|11\rangle$ となるように $\chi L = \pi$ と置く．次に 2 つの 2 重軌道状態，つまり 4 つの光モードを考える．これらは 4 つの基底状態 $|e_{00}\rangle = |1001\rangle$, $|e_{01}\rangle = |1010\rangle$, $|e_{10}\rangle = |0101\rangle$, $|e_{11}\rangle = |0110\rangle$ が張る空間に存在する．便宜上最初の 2 つの対の通常の順序を入れ換えてあることを注意しておく（物理的にはこの 2 モードは反射鏡を使って容易に入れ換えられる）．真ん中の 2 モードに対して Kerr 媒質が作用すると，$K|e_{11}\rangle = -|e_{11}\rangle$ 以外はすべての $i$ に対して $K|e_i\rangle = |e_i\rangle$ となる．こうすると制御 NOT 演算が次のように因数分解されるので便利である：

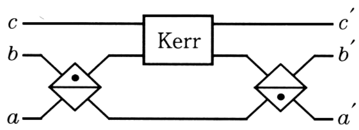
$$\underbrace{\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}}_{U_{CN}} = \underbrace{\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix}}_{I\otimes H} \underbrace{\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}}_{K}$$
$$\underbrace{\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix}}_{I\otimes H}, \tag{7.46}$$

ここで $H$ は単一 q ビット Hadamard 変換（ビームスプリッタと位相シフタで容易に実現できる），$K$ はいま述べた $\chi L = \pi$ に対する Kerr 相互作用である．コラム 7.4 で述べるように，このような装置は可逆な古典的光論理ゲートを構成するために前に考えたことがある．これが単一光子領域で量子論理ゲートとして働く．

まとめると，Kerr 媒質を使って制御 NOT を構成することができて，任意の q ビット演算はビームスプリッタと位相シフタで実現できる．単一光子はレーザ光を減衰させると得られ，光検出器で検出できる．したがって，理論上はこれらの光部品を用いて量子コンピュータを実現できる！

### コラム 7.4: 量子光学的 Fredkin ゲート

光 Fredkin ゲートは次の模式図に示すように，2 つのビームスプリッタと非線形 Kerr 媒質で構築できる：




これはユニタリー変換 $U = B^\dagger K B$ を実行する．ここで $B$ は 50/50 のビームスプリッタ，$K$ は Kerr 相互位相変調オペレータ $K = e^{i\xi b^\dagger b c^\dagger c}$，$\xi = \chi L$ は結合係数と相互作用距離の積である．これを簡単にすると

$$U = \exp\left[i\xi c^\dagger c\left(\frac{b^\dagger - a^\dagger}{2}\right)\left(\frac{b-c}{2}\right)\right] \tag{7.47}$$

$$= e^{i\frac{\pi}{2}b^\dagger b} e^{\frac{\xi}{2}c^\dagger c(a^\dagger b - b^\dagger a)} e^{-i\frac{\pi}{2}b^\dagger b} e^{i\frac{\xi}{2}a^\dagger a c^\dagger c} e^{i\frac{\xi}{2}b^\dagger b c^\dagger c}. \tag{7.48}$$

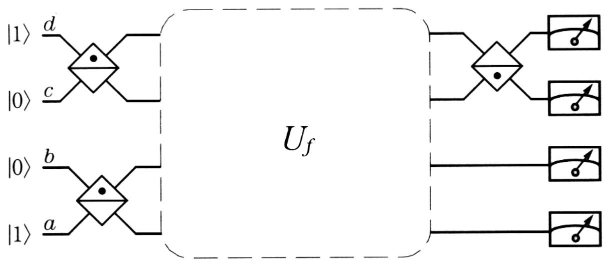
第 1 と第 3 の指数関数は一定の位相シフト，最後の 2 つの位相シフトは相互位相変調による．これらはすべて基本的なものではなく補償できる．興味あるのは第 2 の因子でありこれが量子 Fredkin オペレータを定義する：

$$F(\xi) = \exp\left[\frac{\xi}{2}c^\dagger c(a^\dagger b - b^\dagger a)\right]. \tag{7.49}$$

通常の（古典的）Fredkin ゲート演算は $\xi = \pi$ の場合に得られ，$c$ に光子入力がなければ $a' = a, b' = b$ であるが，$c$ に単一光子が入ると $a' = b, b' = a$ となる．$F(\xi)$ はいわば制御ビームスプリッタ オペレータのようなもので，回

転角が $\xi c^\dagger c$ であると認識すれば理解できる．ここの表現では 2 重軌道表現を使っていないことに注意する．2 重軌道の表現ならばこの Fredkin ゲートは制御 NOT ゲートに相当する．

**演習 7.13:（光学的 Deutsch-Jozsa 量子回路）** 1.4.4 項（第 I 巻）において 1 ビットの Deutsch-Jozsa の問題を解く量子回路について述べた．ビームスプリッタ，位相シフタ，非線形 Kerr 媒質を使った（2 重軌道表現の）単一光子状態に対する Deutsch-Jozsa の量子回路を示す：




(1) Fredkin ゲートとビームスプリッタを使って 4 つの可能な古典的関数 $U_f$ に対する回路を構築せよ．

(2) この構成でなぜ位相シフタが必要ないのか？

(3) 如何に量子アルゴリズムが働くかを説明するために，如何に干渉が使われるかを，各 $U_f$ に対して明示的に説明せよ．

(4) これを実行する際に，単一光子状態をコヒーレント状態で置き換えても動作するか？

**演習 7.14:（古典的な相互位相変調器）** Kerr 媒質の古典的振る舞いが $K$ の定義 (7.41) から期待通り得られるかどうかを見るために，この式を 2 つのモード，つまり 1 つはコヒーレント状態，もう 1 つは状態 $|n\rangle$ に適用せよ．つまり次式を示せ：

$$K|\alpha\rangle|n\rangle = |\alpha e^{i\chi L n}\rangle|n\rangle. \tag{7.50}$$

これを使って

$$\rho_a = \mathrm{tr}_b\Big[K|\alpha\rangle|\beta\rangle\langle\beta|\langle\alpha|K^\dagger\Big] \tag{7.51}$$

$$= e^{-|\beta|^2}\sum_m \frac{|\beta|^{2m}}{m!}|\alpha e^{i\chi Lm}\rangle\langle\alpha e^{i\chi Lm}| \tag{7.52}$$

を計算し，総和への主たる寄与は $m = |\beta|^2$ により生じることを示せ．

### 7.4.3 欠 点

単一光子表現の q ビットは魅力的である．単一光子を発生したり測定するのは比較的簡単であり，2 重軌道表現で任意の単一 q ビット演算が可能である．残念ながら光子の相互作用が困難であり，得られる最良の非線形 Kerr 媒質でも非常に弱く単一光子間で $\pi$ の相互位相変調ができない．実際非線形屈折率は光共鳴に近い媒質を用いて得られるので非線形性にはなにがしかの吸収を伴い，理論的推定によれば最良の配置でも，各光子が $\pi$ の相互位相変調を受けるには約 50 個の光子が吸収されねばならない．従来の非線形光部品で量子コンピュータを構築する見通しは，最良でも僅かしかないことを意味している．

それにもかかわらずこの光子による量子コンピュータの研究から，量子コンピュータ**構成**の性格とシステム設計に関して価値ある見通しが得られる．いまや実験室段階で（もし十分良い部品だけが使えるとしても）実際の量子コンピュータがどのようなものかを知ることができ，光干渉計によってほとんど完全に構成できるのが印象的である．この装置では情報が光子数と光子の位相の両方に符号化され，干渉計が 2 つの表現の間を変換する．安定な光干渉計を作るのは容易であるが，もし代わりに q ビットとして質量を持つ表現を選ぶと典型的 de Broglie 波長が短いので，安定な干渉計を作るのは急速に困難になる．光の表現でも大きな量子アルゴリズムを実現するには相互に結合した干渉計が多数必要になり，その安定化は実験室でも困難な問題となる．

歴史的に**古典的**光コンピュータが電子的装置に代わり得る有望株と考えられたこともあるが，十分に非線形な光材料が発見されず，速度と並列性の利点が調整と電力消費の欠点を補えなかったので，結局は期待に沿えなかった．他方で光通信は極めて重要な領域となった．この理由の 1 つは 1cm 以上の距離においてファイバを通じて光子を使って 1 ビットを伝送するに要するエネルギーは，同じ長さを

カバーする典型的な 50Ω の伝送路を充電するに要するエネルギーよりも少ない．同様に光 q ビットも計算よりは，量子暗号におけるような量子情報の通信で本領を発揮するかも知れない．

光子による量子コンピュータの実現が困難に直面しているにもかかわらず，これらを記述する理論的形式は，無条件で本章でこれから調べていく他の物理的実現法の基礎となる．次に述べるのは光子の量子コンピュータのもう 1 つの種類では，実際に異なる（そしてより良い）非線形媒質を用いている．

**光子による量子コンピュータ**

- **q ビット表現：** 2 つのモード $|01\rangle$, $|10\rangle$ における単一光子の存在，または偏光．
- **ユニタリー時間発展：** 位相シフタ（$R_z$ 回転），ビームスプリッタ（$R_y$ 回転）および 2 つの単一光子を相互位相変調させて $\exp[i\chi L|11\rangle\langle 11|]$ を実行する非線形 Kerr 媒質を用いて，任意のユニタリー変換を構築する．
- **初期状態の作成：** 単一光子状態の生成（例えばレーザ光の減衰による）．
- **読み出し：** 単一光子を検出（例えば光電子増倍管を使う）．
- **欠点：** 相互位相変調指数と吸収損失の比が大きな非線形 Kerr 媒質を実現するのが困難．

## 7.5　光共振器量子電気力学

**共振器量子電気力学**(共振器 QED，cavity quantum electrodynamics) では単一原子と少数の光モードとの結合を含む重要な領域を研究する．実験的には単一原子を Q 値が非常に高い光共振器中に置くことによりこの結合が可能になる．1 つまたは 2 つの電磁波モードしか共振器内に存在せず，その各々が非常に高い電界強度を持つので，原子と電界の間の電気双極子結合が高まる．Q 値が高いために共振器中の光子は外に出る前に原子と何度も相互作用する機会を持つ．理論的にこの技術により単一量子システムを制御して研究する機会が生まれ，量子カオス，量子フィードバック制御，量子計算等の多くの分野が開かれる．

特に単一原子共振器 QED 法は前節で述べた光・量子コンピュータのジレンマを解決可能な方法を提供する．単一光子は量子情報の良い担い手であるが，互い

に相互作用するには何か他の媒質を必要とする．従来の非線形 Kerr 媒質はバルク材料なのでこの要請を満たすことはできない．しかし，十分に孤立化した単一原子ならば必ずしもコヒーレンスの劣化を起こさずに，光子間の相互位相変調を起こせるかも知れない．実際に単一光子状態が単一原子と効率的にやり取りができて，その相互作用が制御できるとしたらどうだろうか？ この筋書きの可能性が本節の話題である．

### 7.5.1　物理的装置

共振器 QED システムの実験上の主な構成要素は電磁界共振器と原子の 2 つである．共振器モードに関する基礎的物理を述べることから始めて，原子構造と原子と光の相互作用についての基礎概念をまとめる．

**Fabry-Perot 共振器**

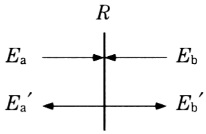
共振器 QED に含まれる主な相互作用は電気双極子モーメント $\vec{d}$ と電界 $\vec{E}$ の間の双極子相互作用 $\vec{d}\cdot\vec{E}$ である．この相互作用の大きさをどれくらいにできるであろうか？ 実際上 $\vec{d}$ の大きさを変えることは難しい．しかし $|\vec{E}|$ は実験的に制御可能であり，狭い周波数帯域でしかも小さな空間的体積で非常に大きな電界を実現する，最も重要なツールが Fabry-Perot 共振器である．

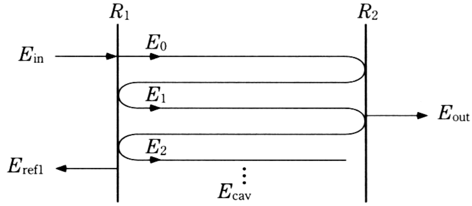
**コラム 7.5: Fabry-Perot 共振器**

Fabry-Perot 共振器の基本的部品は部分的に反射する反射鏡である．これによって入射光 $E_a$ と $E_b$ が部分的に反射・透過をして出力電界 $E_{a'}$ と $E_{b'}$ を作り出す．これらの関係はユニタリー変換であり：

$$\begin{bmatrix} E_{a'} \\ E_{b'} \end{bmatrix} = \begin{bmatrix} \sqrt{R} & \sqrt{1-R} \\ \sqrt{1-R} & -\sqrt{R} \end{bmatrix} \begin{bmatrix} E_a \\ E_b \end{bmatrix}, \tag{7.53}$$

ここで $R$ は反射鏡の反射率，「$-$」符号の位置は便宜上慣用に従った．




Fabry-Perot 共振器は反射率 $R_1$, $R_2$ の 2 枚の平行平面鏡より成り，図に示すように光 $E_{in}$ が外部から入射する．共振器内部では 2 枚の反射鏡間を光が往復し，1 往復毎に位相シフト $e^{i\varphi}$ が生じる．ここで $\varphi$ は行路長と光の周波数の関数である．したがって，式 (7.53) を使うと共振器内部の電界は：

$$E_{cav} = \sum_k E_k = \frac{\sqrt{1-R_1}E_{in}}{1+e^{i\varphi}\sqrt{R_1R_2}}, \tag{7.54}$$

ここで $E_0 = \sqrt{1-R_1}E_{in}$, $E_k = -e^{i\varphi}\sqrt{R_1R_2}E_{k-1}$ である．同様に $E_{out} = e^{i\varphi/2}\sqrt{1-R_2}$, $E_{refl} = \sqrt{R_1}E_{in} + \sqrt{1-R_1}\sqrt{R_2}e^{i\varphi}E_{cav}$ であることがわかる．

我々の目的にとって重要な Fabry-Perot 共振器の性質は，入力電力と周波数の関数としての共振器の内部電界の電力である：

$$\frac{P_{cav}}{P_{in}} = \left|\frac{E_{cav}}{E_{in}}\right|^2 = \frac{1-R_1}{|1+e^{i\varphi}\sqrt{R_1R_2}|^2}. \tag{7.55}$$

2 つの側面に注目する．第 1 に $\varphi = \omega d/c$ によって周波数選択性が現れる．ここで $d$ は反射鏡間隔，$c$ は光速，$\omega$ は電界周波数である．物理的にこれは共振器電界と前面反射鏡で反射した光との同位相もしくは逆位相の干渉で生じる．第 2 は共振時に共振器電界は入射電界のほぼ $1/(1-R)$ 倍の最大値をとる．この性質が共振器 QED にとって重要である．

電界が単色で単一の空間モードを占めると近似すると，量子力学的記述が簡単になる：

$$\vec{E}(r) = i\vec{\epsilon}E_0\left[ae^{ikr} - a^\dagger e^{-ikr}\right]. \tag{7.56}$$

コラム 7.5 で述べたように，これらの近似は Fabry-Perot 共振器内の電界に対し

て成り立つ．ここで $k = \omega/c$ は光の空間周波数，$E_0$ は電界強度，$\vec{\epsilon}$ は偏光，$r$ は必要とする電界の位置である．$a$ と $a^\dagger$ はモードの光子に対する消滅と生成のオペレータである．共振器電界の時間発展を規定する Hamiltonian は簡単に

$$H_{\rm field} = \hbar\omega a^\dagger a \tag{7.57}$$

であり，これはエネルギーが共振器中の $|\vec{E}|^2$ の体積積分であるという半古典的概念と一致する．

**演習 7.15:** $R_1 = R_2 = 0.9$ に対して共振器中の電力式 (7.55) を電磁界位相のずれ $\varphi$ の関数としてグラフに描け．

### 2 準位原子

これまで光子のみ，あるいは半古典的媒質に仲介された光子間の相互位相変調のような相互作用を議論してきた．ここで原子に注意を向けてその電子的性質と光子との相互作用を議論する．もちろんこれは非常に奥深くまた高度に発展した研究分野であり，量子計算に関連する僅かな部分を述べるに留める．

原子の電子的エネルギー固有状態は非常に複雑であるが（コラム 7.6 参照），原子が 2 つの準位のみを持つとする原子モデルは我々の目的にとって優れた近似である．この **2 準位原子近似**(two-level atom approximation) が成り立つ理由は単色光との相互作用のみを扱うことと，次の 2 つの条件を満たすエネルギー準位だけが関連するからである．つまりエネルギー差が入射光子のエネルギーに一致することと，対称性（「選択則」）が遷移を禁止しないことである．これらの条件はエネルギー，角運動量およびパリティの基本的保存則から生じる．エネルギー保存は次の条件である：

$$\hbar\omega = E_2 - E_1, \tag{7.58}$$

ここで $E_2$ と $E_1$ は原子の 2 つの固有エネルギーである．角運動量とパリティ保存条件は，2 つの軌道の波動関数間の $\hat{r}$ の行列要素 $\langle l_1, m_1|\hat{r}|l_2, m_2\rangle$ を考えると示すことができる．一般性を失うことなく $\hat{r}$ は $\hat{x}-\hat{y}$ 面内にあるとして，球面調和関数（コラム 7.6）で次のように表現できる：

$$\hat{r} = \sqrt{\frac{3}{8\pi}}\left[(-r_x + ir_y)Y_{1,+1} + (r_x + ir_y)Y_{1,-1}\right]. \tag{7.59}$$

この基底によると $\langle l_1, m_1|\hat{r}|l_2, m_2\rangle$ に関連する項は：

$$\int Y^*_{l_1 m_1} Y_{1m} Y_{l_2 m_2} d\Omega. \tag{7.60}$$

$m = \pm 1$ を思い出すと，この積分が 0 でないのは $m_2 - m_1 = \pm 1$ と $\Delta l = \pm 1$ のときのみである．$\langle l_1, m_1|\hat{r}|l_2, m_2\rangle$ が関与する双極子近似において，第 1 の条件が角運動量保存，第 2 がパリティ保存である．これらの条件が 2 準位原子近似において重要な選択則を与える．

## コラム 7.6: 原子のエネルギー準位

原子中の電子は 3 次元箱中の粒子のように振る舞い，次の Hamiltonian で記述される：

$$H_A = \sum_k \frac{|\vec{p}_k|^2}{2m} - \frac{Ze^2}{r_k} + H_{\rm rel} + H_{\rm ee} + H_{\rm so} + H_{\rm hf}, \tag{7.61}$$

ここで最初の 2 項は電子の運動エネルギーと，電子の負電荷と核の正電荷間の引力のバランスを記述し，$H_{\rm rel}$ は相対論的補正項，$H_{\rm ee}$ は電子・電子の結合と電子のフェルミ粒子的性質の寄与，$H_{\rm so}$ は電子スピンが原子を巡る電子軌道で作られる磁界と相互作用すると考えられるスピン・軌道相互作用，$H_{\rm hf}$ は電子スピンが核の作る磁界と相互作用する超微細構造を表す．$H_A$ のエネルギー固有状態は 3 つの整数または半整数の**量子数**（quantum number），つまり主量子数 $n$，軌道角運動量 $l$，その $\hat{z}$ 成分 $m$ によってかなりよく分類できる．これに加えて全電子スピン $S$，核スピン $I$ も重要である．$H_A$ の固有値は $\alpha^2$ のオーダで $n$ によってほぼ決まり，それより少し小さいオーダで $H_{\rm ee}$，$\alpha^4$ のオーダで $H_{\rm rel}$ と $H_{\rm so}$，$\approx 10^{-3}\alpha^4$ のオーダで $H_{\rm hf}$ によって決まる．ここで $\alpha = 1/137$ は無次元の**微細構造定数**(fine structure constant) である．

主量子数 $n$ の導出は簡単であり Coulomb の閉じ込めポテンシャルは半径方向の距離のみに依存するので，箱の中の粒子に対する通常の 1 次元 Schrödinger 方程式の解に従う．しかし軌道角運動量は 3 次元の性質を持つので少し説明を要する．重要な性質は $H_A$ を座標表現したときの角度依存性から生じ，$\vec{p}$

が Laplace オペレータ $\vec{\nabla}^2$ で表されて次の Schrödinger 方程式を与える：

$$\frac{\Phi(\varphi)}{\sin\theta}\frac{d}{d\theta}\left(\sin\theta\frac{d\Theta}{d\theta}\right)+\frac{\Theta(\theta)}{\sin^2\theta}\frac{d\Phi(\varphi)}{d\varphi^2}+l(l+1)\Theta(\theta)\Phi(\varphi)=0, \tag{7.62}$$

ここで $\theta$ と $\varphi$ は通常の球面座標，$\Phi$ と $\Theta$ は我々が望む固有関数である．解 $Y_{lm}(\theta,\varphi)=\Theta_{lm}(\theta)\Phi_m(\varphi)$ は**球面調和関数**(spherical harmonics) である：

$$Y_{lm}(\theta,\ \varphi)\equiv(-1)^m\sqrt{\frac{2l+1}{4\pi}\frac{(l-m)!}{(l+m)!}}P_{lm}(\cos\theta)e^{im\varphi}, \tag{7.63}$$

ここで $P_{lm}$ は通常の Legendre 関数である：

$$P_{lm}(x)=\frac{(1-x^2)^{m/2}}{2^l l!}\frac{d^{m+l}}{dx^{m+l}}(x^2-1)^l. \tag{7.64}$$

これらの式において $-l\le m\le l$ であり，$m$ と $l$ は整数または半整数である．$l$ を軌道角運動量と呼び，$m$ はその $\hat{z}$ 軸方向成分である．同様に電子スピン $S$ と角スピン $I$ も成分 $m_s$ と $m_i$ を持っている．これでわかるように原子エネルギー状態は極めて複雑である！ まとめると，我々の目的には原子の固有状態は，7 つの数 $n,\ l,\ m,\ S,\ m_s,\ I,\ m_i$ で決まると考えてよい．

**演習 7.16:（電気双極子の選択則）**　式 (7.60) がゼロでないのは $m_2-m_1=\pm1$ と $\Delta l=\pm1$ のときのみであることを示せ．

実際に光が**完全**に単色であることはない．光がレーザのような光源で発生するときに縦モードや励起雑音その他の原因で有限の線幅を持つ．また外界と結合する原子も**完全**に定義されたエネルギー準位を持つことはない．近くの電気的ポテンシャルの揺らぎあるいは真空との相互作用によってさえも，各エネルギー準位はぼやけて有限の幅で分布するようになる．

それにもかかわらず，原子と励起エネルギーを注意深く選んで選択則を利用すれば，2 準位原子近似が十分成立する状況が作れる．この手続きの全体像は次のようになる．この近似で 2 つの選んだ準位を $|\psi_1\rangle$ と $|\psi_2\rangle$ とすると，$\hat{r}$ の行列要素は：

$$r_{ij} = \langle \psi_i | \hat{r} | \psi_j \rangle \approx r_0 Y, \tag{7.65}$$

ここで $r_0$ はある定数，$Y$ は Pauli のオペレータである（2.1.3 項参照：第 I 巻．$X$ の代わりに $Y$ を用いたのは実際上重要でない．これは慣用上と後の計算の便宜上の問題である）．これは原子と入射電界の相互作用を記述する際に関係してくる．この 2 準位部分空間における原子自体の Hamiltonian は簡単に：

$$H_{\text{atom}} = \frac{\hbar\omega_0}{2} Z. \tag{7.66}$$

ここで 2 つの状態はエネルギー固有状態なので，$\hbar\omega_0$ は 2 準位のエネルギー差である．

### 7.5.2　Hamiltonian

原子と共振器に閉じ込められた電界間の双極子相互作用 $\vec{d} \cdot \vec{E}$ は，もっと簡単なモデルで十分良い近似ができる．ここでは原子の 2 準位近似と，共振器電界の量子化，および電子サイズが電界の波長に比べて十分に小さいことを使う．$\vec{d} \propto \hat{r}$（電気双極子の大きさは電荷と距離の積）という事実を使って式 (7.56) と式 (7.65) を組み合わせると：

$$H_I = -igY(a - a^\dagger), \tag{7.67}$$

ここで原子が置かれた位置（したがって，電界 $\vec{E}$ を計算する位置）を $r = 0$ と選び，$\hat{r}$ が電界ベクトルとそろうように原子を配置する．$g$ は相互作用の強さを記述する定数である（ここでは具体的値を知る必要はなく，形だけわかればよい）．$i$ が入っているのは，$H_I$ が Hermite オペレータでなければならず $g$ を実数にするためである．$H_I$ には一般に微小な項が含まれるので，これを見るために Pauli の上昇，下降オペレータ：

$$\sigma_\pm = \frac{X \pm iY}{2} \tag{7.68}$$

を導入して $H_I$ を書き換える：

$$H_I = g(\sigma_+ - \sigma_-)(a - a^\dagger). \tag{7.69}$$

$\sigma_+ a^\dagger$ と $\sigma_- a$ を含む項はいま考えている周波数 $\omega$ と $\omega_0$ の 2 倍の周波数で振動するので，これを無視してもかなり良い近似になる（**回転波近似**(rotating wave approximation)）．全 Hamiltonian $H = H_{\text{atom}} + H_{\text{field}} + H_I$ は，

$$H = \frac{\hbar\omega_0}{2} Z + \hbar\omega a^\dagger a + g(a^\dagger \sigma_- + a\sigma_+). \tag{7.70}$$

繰り返すと，ここでも Pauli のオペレータは 2 準位原子に働き，$a^\dagger, a$ は単一モード電界の上昇，下降オペレータ，$g$ は原子と電界の相互作用の結合係数である．これが共振器 QED 研究の基本的な理論ツールである **Jaynes-Cummings** の Hamiltonian であり，2 準位原子と電磁界の相互作用を記述する．

$N = a^\dagger a + Z/2$ が運動の定数，つまり $[H, N] = 0$ であることに留意すると，この Hamiltonian は別の便利な形に書き直せる：

$$H = \hbar\omega N + \delta Z + g(a^\dagger \sigma_- + a\sigma_+), \tag{7.71}$$

ここで $\delta = (\omega_0 - \omega)/2$ を**離調**(detuning) — 電界と原子共鳴の周波数差 — と呼ぶ．この Hamiltonian，つまり Jaynes-Cummings の Hamiltonian は非常に重要であり，本章の残りのほとんどすべてでその性質と異なる物理システムへの適用について調べる．

**演習 7.17:（Jaynes-Cummings の Hamiltonian の固有状態）** $\omega = \delta = 0$ に対して

$$|\chi_n\rangle = \frac{1}{\sqrt{2}}\left[|n,\ 1\rangle + |n+1,\ 0\rangle\right], \tag{7.72}$$

$$|\bar{\chi}_n\rangle = \frac{1}{\sqrt{2}}\left[|n,\ 1\rangle - |n+1,\ 0\rangle\right], \tag{7.73}$$

は Jaynes-Cummings の Hamiltonian (7.71) の固有状態であり，固有値が

$$H|\chi_n\rangle = g\sqrt{n+1}|\chi_n\rangle, \tag{7.74}$$

$$H|\bar{\chi}_n\rangle = -g\sqrt{n+1}|\bar{\chi}_n\rangle, \tag{7.75}$$

であることを示せ．ここでケット記号は $|$ 電界, 原子 $\rangle$ を表す．

### 7.5.3　単一光子・単一原子の吸収と屈折

我々の目的にとって最も興味深い共振器 QED の構成は**単一の**光子が**単一の**原子と相互作用するものである．通常とは異なるこのような領域では，古典的電磁

気学の従来の（屈折率や誘電率のような）概念は成立しない．我々は特に単一原子を利用して光子間に非線形の相互作用を生じさせる．

**Rabi 振動**(Rabi oscillation) と呼ぶ原子・電界システムにおける顕著で一般的な特性を示すことから始める．$N$ は固定位相を与えるだけなので無視しても一般性を失うことはない．時間発展が $U = e^{-iHt}$ で与えられ（$\hbar$ を落とすのが便利なことがあるので，これ以降自由に行う），電界モードでたかだか単一の光子が励起される場合に話を限ると

$$H = -\begin{bmatrix} \delta & 0 & 0 \\ 0 & \delta & g \\ 0 & g & -\delta \end{bmatrix}, \tag{7.76}$$

（基底状態は左から右へ，上から下へ向かって $|00\rangle, |01\rangle, |10\rangle$ である．ここで左の記号が電界，右が原子を示す．）時間発展は

$$\begin{aligned} U &= e^{-i\delta t}|00\rangle\langle 00| \\ &\quad + \left(\cos\Omega t + i\frac{\delta}{\Omega}\sin\Omega t\right)|01\rangle\langle 01| + \left(\cos\Omega t - i\frac{\delta}{\Omega}\sin\Omega t\right)|10\rangle\langle 10| \\ &\quad -i\frac{g}{\Omega}\sin\Omega t\Big(|01\rangle\langle 10| + |10\rangle\langle 01|\Big). \end{aligned} \tag{7.77}$$

興味深い振る舞いをするのはこの式の最後の行であり，これにより原子と電界はエネルギー量子をやり取りしながら **Rabi 周波数**(Rabi frequency) $\Omega = \sqrt{g^2 + \delta^2}$ で振動する．

**演習 7.18:（Rabi 振動）**　$H$ を指数関数化するために

$$e^{i\hat{n}\cdot\vec{\sigma}} = \cos|n| + i\hat{n}\cdot\vec{\sigma}\sin|n| \tag{7.78}$$

を使って式 (7.77) が正しいことを示せ．これは非常に簡単な Rabi 振動と Rabi 周波数の導出法である．通常は連立微分方程式を解いて $\Omega$ を求めるが，ここでは単一原子，単一光子の部分空間に注目して，本質的なダイナミクスを得ている！

単一原子と相互作用をしている単一光子の変換は原子状態についてトレースをとることにより得られる（2.4.3 項：第 I 巻）．初期状態の光子 $|1\rangle$ が（初期状態が

基底状態 $|0\rangle$ にある）原子に吸収される確率は簡単に次式で与えられる：

$$\chi_r = \sum_k |\langle 0k|U|10\rangle|^2 = \frac{g^2}{g^2+\delta^2}\sin^2\Omega t. \tag{7.79}$$

これは共鳴からの離調 $\delta$ の関数として吸収に期待される通常の Lorentz 型の分散曲線である．

屈折率（単一原子の！）は原子が基底状態にあるときの $U$ の行列要素で与えられる．光子が受ける位相シフトは，電界状態が $|1\rangle$ と $|0\rangle$ のときに受ける回転角の差を原子に関してトレースをとったものであり，次式で与えられる：

$$\chi_i = \arg\left[e^{i\delta t}\left(\cos\Omega t - i\frac{\delta}{\Omega}\sin\Omega t\right)\right]. \tag{7.80}$$

結合 $g$ が減少するとゼロでない一定の $\delta$ に対して，吸収確率 $\chi_r$ は $g^2$ と共に減少するが位相シフト $\chi_i$ はほぼ一定に保たれる．これはあまり光を散乱することなく位相シフトを起こす材料の起源となる．

**演習 7.19:（Lorentz 型吸収プロフィール）** $t=1$, $g=1.2$ に対して離調 $\delta$ の関数として式 (7.79) と（もし知っていれば）対応する古典的結果をプロットせよ．振動の原因は何か？

**演習 7.20:（単一光子の位相シフト）** $U$ から式 (7.80) を導き，$t=1$, $g=1.2$ に対して離調 $\delta$ の関数としてプロットして，$\delta/\Omega^2$ と比較せよ．

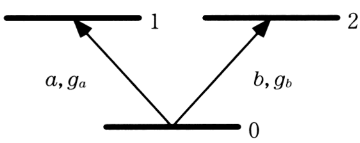



**図 7.4:** オペレータ $a$, $b$ で記述される 2 つの直交した偏光と相互作用する 3 準位原子（準位 0, 1, 2）．原子・光子間の結合はそれぞれ $g_a$ と $g_b$ である．0 と 1，0 と 2 の間のエネルギー差はほとんど等しいとする．

原子・光子間相互作用の自然な応用として，2 つの異なる光子モード（各モードにたかだか 1 つの光子が含まれる）が同じ原子と相互作用するときに何が起きるかを調べる．これによって 2 モード間に非線形相互作用が起こり得る．7.4.2 項

で非線形 Kerr 媒質は $H = \chi a^\dagger a b^\dagger b$ の形の Hamiltonian で相互位相変調を起こす媒質として現象論的に述べた．そこではこの効果が基礎的相互作用から如何に生じるかは見なかった．いまの定式化から Kerr 効果の起源が図 7.4 に示す 3 準位原子において，2 つの偏光が相互作用する簡単なモデルで説明できる．これは変形した Jaynes-Cummings の Hamiltonian で記述される．

$$H = \delta \begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} + g_a \left( a \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} + a^\dagger \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \right) + g_b \left( b \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix} + b^\dagger \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \right), \tag{7.81}$$

ここで $3 \times 3$ 原子オペレータの基底要素は $|0\rangle$, $|1\rangle$, $|2\rangle$ である．行列形式で $H$ の関連する項はブロック対角行列で表される．

$$H = \begin{bmatrix} H_0 & 0 & 0 \\ 0 & H_1 & 0 \\ 0 & 0 & H_2 \end{bmatrix}, \tag{7.82}$$

ここで

$$H_0 = -\delta \tag{7.83}$$

$$H_1 = \begin{bmatrix} -\delta & g_a & 0 & 0 \\ g_a & \delta & 0 & 0 \\ 0 & 0 & -\delta & g_b \\ 0 & 0 & g_b & \delta \end{bmatrix} \tag{7.84}$$

$$H_2 = \begin{bmatrix} -\delta & g_a & g_b \\ g_a & \delta & 0 \\ g_b & 0 & \delta \end{bmatrix}. \tag{7.85}$$

基底状態は $H_0$ に対して $|a,\ b,\ \text{原子}\ \rangle = |000\rangle$，$H_1$ に対して（左列から右に）$|100\rangle$, $|001\rangle, |010\rangle$, $|002\rangle$，$H_2$ に対して $|110\rangle$, $|011\rangle$, $|102\rangle$ である．指数関数化して $U = \exp(iHt)$ とすると，単一光子位相シフト

$$\varphi_a = \arg(\langle 100|U|100\rangle) - \arg(\langle 000|U|000\rangle),$$

$$\varphi_b = \arg(\langle 010|U|010\rangle) - \arg(\langle 000|U|000\rangle)$$

と 2 光子位相シフト

$$\varphi_{ab} = \arg(\langle 110|U|110\rangle) - \arg(\langle 000|U|000\rangle)$$

が求まる．線形媒質ならば $\varphi_{ab} = \varphi_a + \varphi_b$，つまり

$$\exp[-i\omega(a^\dagger a + b^\dagger b)]|11\rangle = \exp(-2i\omega)|11\rangle$$

なので，2 光子状態は単一光子状態の 2 倍の位相シフトが期待される．しかし，このシステムは非線形の振る舞いを示し，図 7.5 に示すように $\chi_3 \equiv \varphi_{ab} - \varphi_a - \varphi_b$ となる．この物理システムで原子が 2 つの光モード間で量子を交換する Kerr 効果が僅かな振幅から生じる．

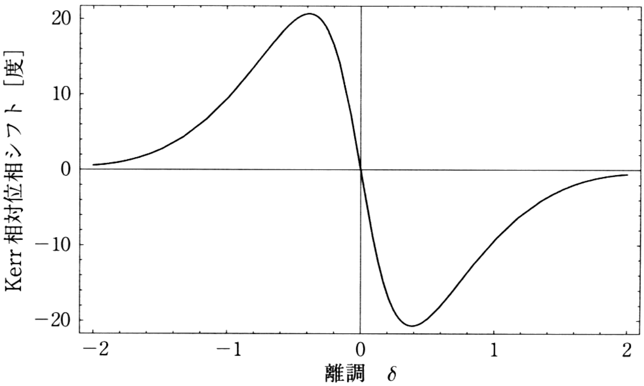



**図 7.5:** $t = 0.98$, $g_a = g_b = 1$ に対して離調 $\delta$ の関数として式 (7.82) から求めた 3 準位原子と相互作用する単一光子の Kerr 位相シフト $\chi_3$（度）．

**演習 7.21:** 式（7.82) を指数関数化して次式を示せ．

$$\varphi_{ab} = \arg\left[e^{i\delta t}\left(\cos\Omega' t - i\frac{\delta}{\Omega'}\sin\Omega' t\right)\right], \tag{7.86}$$

ここで $\Omega' = \sqrt{\delta^2 + g_a^2 + g_b^2}$ である．これを使って非線形 Kerr 位相シフト $\chi_3$ を計算せよ．これは古典的非線形光学に典型的に含まれる多くの複雑な

取り扱いを避けて，Kerr 相互作用をモデル化して理解するのに非常に簡単な方法である．

**演習 7.22:** 相互位相変調にはある一定量の損失を伴い，それは光子が原子により吸収される確率で与えられる．この確率 $1 - \langle 110|U|110\rangle$ を計算せよ．ただし式 (7.82) で与えられる $H$ に対して $U = \exp(-iHt)$ である．また $\delta$, $g_a$, $g_b$, $t$ の関数として $1 - \langle 100|U|100\rangle$ と比較せよ．

### 7.5.4　量子計算

おおまかに言えば共振器 QED 技術を用いるとさまざまな方法で量子計算ができる．そのうちの 2 つを示すと光子状態で量子情報を表現して，原子を含む共振器を用いて光子間の非線形相互作用を行わせるものと，原子で量子情報を表現して原子間を光子で通信するものがある．このうち，最初の方法を使って量子論理ゲートを実現する実験を紹介してこの話題を終える．

7.4.2 項で見たように単一光子状態，位相シフタ，ビームスプリッタおよび非線形 Kerr 媒質を用いて量子コンピュータを構築できるが，制御 NOT ゲートを作り出すのに必要な $\pi$ の相互位相変調は，標準的なバルク非線形光学材料を以ててしてはほとんど実現不可能に近い．7.5.3 項で示したように共振器 QED を用いて Kerr 相互作用が実行ができる．バルク媒質と異なり Fabry-Perot 型共振器で強い電界が作られるので，これは単一光子レベルでも強い効果をもたらす．

ユニタリー変換：

$$
\begin{bmatrix}
1 & 0 & 0 & 0 \\
0 & e^{i\varphi_a} & 0 & 0 \\
0 & 0 & e^{i\varphi_b} & 0 \\
0 & 0 & 0 & e^{i(\varphi_a+\varphi_b+\Delta)}
\end{bmatrix}
\tag{7.87}
$$

の論理ゲートの実現可能性を示すために行われた共振器 QED の実験を図 7.6 に示す（章末の「歴史と参考資料」参照）．ここで単一光子を用いると $\Delta = 16^\circ$ である．実験では弱いコヒーレント状態の 2 モード光（非常に僅かな周波数差で区別する）を準備し，一方は直線偏光（プローブ）他方は円偏光（ポンプ）として

共振器に入射する．直線偏光が右回りと左回りの 2 つの円偏光状態（+ と −）の重ね合せで表せることを思い出すと，この状態は次のように書ける：

$$|\psi_{\text{in}}\rangle = |\beta^+\rangle \left[ \frac{|\alpha^+\rangle + |\alpha^-\rangle}{\sqrt{2}} \right]. \tag{7.88}$$

弱いコヒーレント状態を $|\alpha\rangle \approx |0\rangle + \alpha|1\rangle$ で近似し，$\beta$ も同様とすると（当面正規化係数は別として）：

$$|\psi_{\text{in}}\rangle \approx \left[|0^+\rangle + \beta|1^+\rangle\right] \ \left[|0^+\rangle + \alpha|1^+\rangle + |0^-\rangle + \alpha|1^-\rangle\right]. \tag{7.89}$$

これらの光子が光共振器に入って原子と相互作用をし，原子が（光子のモードに関係なく）各偏光に対して光子数に依存した異なる位相シフトを引き起こすとモデル化する．具体的には $|1^+\rangle$ 状態がプローブビームにあれば $e^{i\varphi_a}$ の位相シフトを，ポンプビームにあれば $e^{i\varphi_b}$ の位相シフトを受けると仮定する．この単一光子位相シフトに加えて状態 $|1^+1^+\rangle$ では付加的な Kerr 効果による位相シフト $\Delta$ を受けて，$e^{i(\varphi_a+\varphi_b+\Delta)}|1^+1^+\rangle$ となる．また他の状態（と特に他の偏光）は変化を受けない．この振る舞いを引き起こす物理は 7.5.3 項で述べたのと同様であり，ポンプとプローブの相互位相変調を起こすという最終的な効果も同じである．したがって，共振器出力は：

$$\begin{aligned}
|\psi_{\text{out}}\rangle \approx\ & |0^+\rangle \left[|0^+\rangle + \alpha e^{i\varphi_a}|1^+\rangle + |0^-\rangle + \alpha|1^-\rangle\right] \\
& + e^{i\varphi_b}\beta|1^+\rangle \left[|0^+\rangle + \alpha e^{i(\varphi_a+\Delta)}|1^+\rangle + |0^-\rangle + \alpha|1^-\rangle\right] \qquad (7.90) \\
\approx\ & |0^+\rangle|\alpha, \varphi_a/2\rangle + e^{i\varphi_b}\beta|1^+\rangle|\alpha, (\varphi_a+\Delta)/2\rangle, \qquad (7.91)
\end{aligned}$$

ここで $|\alpha, \varphi_a/2\rangle$ は垂直方向から $\varphi_a/2$ だけ回転した直線偏光プローブ電界を表す．電界の偏光は検出器で検出され，$\varphi_a \approx 17.5^\circ$，$\varphi_b \approx 12.5^\circ$ および $\Delta \approx 16^\circ$ を与える．$\Delta$ が有意の値となるので，この結果は単一光子と，それと相互作用する非線形光学 Kerr 媒質としての単一原子を用いて，普遍的な 2 - q ビット論理ゲート（演習 7.23）が可能であることを示唆している．

実験結果を解釈するに当たって注意すべき点が幾つかある．入射光子は共振器と原子を横切る際の吸収確率は無視できないので，実際に実行される量子演算はユニタリーでない．この問題は，例えば（$\Delta = \pi$ が要求される）制御 NOT ゲートに要求されるような，多数ゲートを縦続に接続する場合に大きな問題となる．

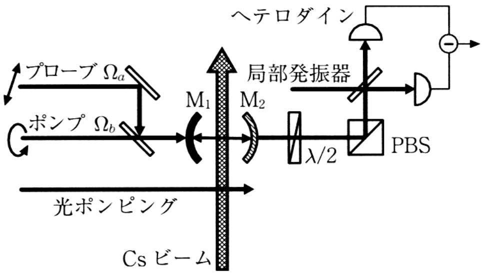



**図 7.6:** 基本的量子論理ゲートとして単一原子を用いて，単一光子間の相互位相変調を起こす可能性を示すために用いられた実験装置の模式図．弱い直線偏光のプローブ光 $\Omega_a$ と強い円偏光のポンプ光 $\Omega_b$ が高反射率の反射鏡 $M_1$，$M_2$ を持つ共振器を照射する．光ポンピングで電子状態 $6\mathrm{S}_{1/2}$，$F = 4$，$m = 4$ に励起されたセシウム原子が平均原子数が 1 に近くなるように共振器中に落ちてくる（図は上下が逆転している）．光は共振器を横切って原子と相互作用する．$\sigma_+$ 円偏光の光が $6\mathrm{P}_{3/2}$，$F' = 5$，$m' = 5$ 状態に強い遷移を，直交した $\sigma_-$ 円偏光が $6\mathrm{P}_{3/2}$，$F' = 5$，$m' = 3$ 状態に弱い遷移を引き起こす．半波長板，偏光ビームスプリッタ（PBS），および（局部発振器で決まる特定波長の光を選択的に検出する）高感度平衡型ヘテロダイン検出器を用いて出力光の偏光を測定する．図は Q. Turchette の厚意による．

実際にこの実験に用いた共振器構成では反射による損失が大きく，共振器をカスケードに配置することが困難である．この問題を解決するためには適切な時間依存モデルを開発し解析する必要がある．また相互位相変調モデルは測定結果と矛盾しないが，光子・原子相互作用モデルは**手始め** (Ansatz) であり，実験で他のモデルを用いることを排除してはいない．実際に実験で（減衰させたコヒーレント状態ではなく）単一光子状態を用いて，$|\psi_{\mathrm{out}}\rangle$ の 2 つのモードのもつれを測定するれば，原理上いいテストになろう．この実験が行われた時点で，量子演算の特性や量子ゲートへの適合性を示す一般的手法は知られていない．しかしこれを行う**プロセストモグラフィー**(process tomography) と呼ぶ方法はよく理解されており（8 章：第 III 巻），注目すべきことに散逸やその他の非ユニタリー的振る舞いを完全に調べることができる．このようなテストを行うことで，ここで述べた実験が実際に量子計算にどの程度まで反映することができるのかを正確に決めることができる．

これらの欠点にもかかわらず，この実験は量子情報処理に要求される基本的概念を示している．Kerr 相互作用のような非線形光学動作が単一光子レベルで実際に起こり，Jaynes-Cummings モデルが本質的に正しいことを証明している．ま

たこの実験は原子と共振器モードのコヒーレント結合率 $g^2/\kappa$ が自由空間へのインコヒーレントな放出率 $\gamma$ より大きい，いわゆる**悪い共振器領域**で行われているが，この結合は入力光子が共振器に出入りする割合よりも弱い．$g > \kappa > \gamma$ となる**強い結合**(strong coupling) の動作領域にすると，より大きな条件付き位相シフト $\Delta$ が得られるかも知れない．

たぶん最も重要なことは，共振器 QED により量子情報処理にとって価値があるその他の豊富な相互作用への扉が開かれる．我々は単一光子と単一原子に焦点を絞って量子情報を展望することにより，共振器 QED の基本的相互作用である Jaynes-Cummings の Hamiltonian を使って，電磁波と物質の相互作用に関する最も基礎的な物理が構築できるのを見てきた．共振器 QED についてはこれで終わりして，次にイオントラップと磁気共鳴を取り上げ，光子・原子間の相互作用，単一原子と単一光子，Jaynes-Cummings の Hamiltonian といった概念を追求する．

**演習 7.23:** 任意の $\varphi_a$，$\varphi_b$ と $\Delta = \pi$ に対して，任意の単一 q ビット演算を加えると，式 (7.87) の 2 - q ビットゲートを使って制御 NOT ゲートが実現できることを示せ．単一 q ビットのユニタリーゲートを加えることで，ほとんどどんな $\Delta$ の値に対してもこのゲートが普遍的になることがわかる．

**光共振器量子電気力学**

- **q ビット表現：** 2 モード $|01\rangle$，$|10\rangle$ 間の単一光子の存在，あるいは偏光．
- **ユニタリー時間発展：** 位相シフタ（$R_z$ 回転），ビームスプリッタ（$R_y$ 回転），および少数原子を含む Fabry-Perot 共振器に光電界を結合させた共振器 QED システムから，任意の変換が構築できる．
- **初期状態の生成：** 単一光子状態を作り出す（例えば減衰させたレーザ光）．
- **読み出し：** 単一光子を検出する（例えば光電子増倍管）．
- **欠点：** 2 光子間の結合は原子によって仲介されるので，共振器内での原子・電界間結合を増すのが望ましい．しかしその場合共振器に対して光子を入出力させるのが難しくなり，ひいては共振器のカスケード配置が制限される．

## 7.6 イオントラップ

本章でこれまで光子を使った q ビット表現について述べてきた．次に原子あるいは原子核の状態を使う表現を扱う．7.1 節で述べたように具体的には電子スピンと核スピンが潜在的に q ビットの良い表現である．スピンは奇妙な（しかし非常に現実的な！）概念である（コラム 7.7）．しかし，異なるスピン状態間のエネルギー差は他の（室温における原子の運動エネルギーのような）エネルギースケールに比べて非常に小さいので，原子のスピン状態は通常観測しづらく，制御するのはさらに困難である．しかし注意深く作られた環境では精巧な制御が可能である．そのような環境で少数の電荷を帯びた原子を電磁トラップに捕獲して孤立させ，その運動エネルギーがスピンエネルギー分布より十分低くなるまで原子を冷却させる．こうすると，単色光を入射して，あるスピン状態を変化させる遷移を選択的に起こさせることができる．これがトラップされたイオンで量子計算を行う方法の本質であり，本節ではこれを扱う．最初に実験装置とその主要部品について概観し，次にシステムをモデル化する Hamiltonian を示す．トラップされた $^9$Be イオンを用いた制御 NOT を実行するために行われた実験について述べ，最後にこの方法の可能性と制約に関して二三のコメントをする．

**演習 7.24:** 磁界中の核スピンのエネルギーはほぼ $\mu_N B$ である．ここで $\mu_N = eh/4\pi m_p \approx 5 \times 10^{-27}$ ジュール/テスラ は核 Bohr 磁子である．$B = 10$ テスラの磁界中の核スピンのエネルギーを計算し，$T = 300\ K$ における熱エネルギー $k_{\rm B}T$ と比較せよ．

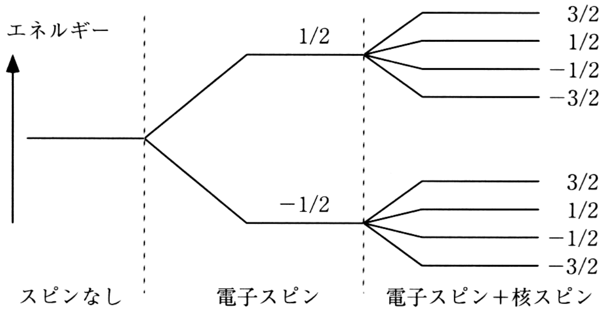
**コラム 7.7: スピン**

スピンは奇妙な概念である．粒子がスピンを持つと，あたかもループ状に流れる電流を持った合成粒子であるかのように磁気モーメントを持つ．しかし電子は素粒子であり，核子を構成するクォークは軌道運動によってスピンを作らない．さらに粒子のスピンは整数か半整数だけしかとらない．

そにもかかわらずスピンは現実的存在であり，日常の物理学においても重要な部分を占める．**ボソン**(boson) と呼ぶ整数スピンの粒子には光子が含まれる．光子は質量がないので特別であってスピン ±1 成分しか持たず（スピ

ンゼロはない)，これがよく知られている2つの直交偏光状態に対応している．安価なプラスティック偏光子で作られたサングラスを通すと，道路のような表面から反射する太陽光が逆偏光方向を持つ部分偏光となるので，ドライブに有効である．(境界面に横向き電界を持つ偏光は入射角によらず部分的に反射するが，これに対し横向き磁界を持つ偏光は入射角が **Brewster** 角のときには反射しない.) **フェルミオン**(fermion) と呼ぶ半整数スピンの粒子には電子，陽子，中性子が含まれる．これらは「スピン 1/2」の粒子であり，スピン成分が +1/2（「上向き」スピン）または −1/2（「下向き」スピン）のいずれかをとる．我々が「スピン」というときはスピン 1/2 の粒子を指すことが多い．

原子エネルギーの固有状態にはスピンや多重スピンの組み合わせが含まれている．例えば $^9$Be の原子核はスピン 3/2 を持っている．磁界と相互作用するスピンは磁気モーメントと同じ振る舞いをする：磁界 $\vec{B}$ 中でスピン $\vec{S}$ を持つ電子はエネルギー $g_e\, \vec{S}\cdot\vec{B}$ を持ち，同様に核スピン $\vec{I}$ はエネルギー $g_n\vec{I}\cdot\vec{B}$ を持つ．例えば，図で描くと原子のエネルギー準位に対するスピンの寄与は次のように見える：




ここではスピン 1/2 の電子とスピン 3/2 の原子核を仮定した．入射レーザの周波数を図の右に合わせると，保存則（7.5.1 項）が満たされる限りこれらのどの遷移でも選択できる．特に角運動量保存則によれば，光子が原子に吸収されると始状態と終状態の間で角運動量またはスピンの 1 ユニットが変化しなければならない．したがって，これらの状態は確定的な角運動量を持たねばならないので，それを考慮に入れる．

連続変数である位置や運動量，あるいは量子ビットを表現するために人為的に縮小しなければならない他の無限 Hilbert 空間システムと異なり，スピン状態は本質的に有限の状態空間に存在するので量子情報の良い表現となる．

### 7.6.1　物理的装置

イオントラップ量子コンピュータの主要部品は，レーザと光検出器を伴う電磁トラップとイオンである．

#### トラップ配置とレーザ

主要な実験装置である電磁トラップは図 7.7 に示すように 4 つの円筒状電極より成っている．電極の両端部分は中心に比べて異なる電圧 $U_0$ にバイアスされ，$\hat{z}$ 軸に沿った静電ポテンシャル $\Phi_{\rm dc} = \kappa U_0[z^2 - (x^2+y^2)/2]$ によって軸方向に閉じ込める（$\kappa$ は幾何学的因子である）．しかし **Earnshaw の定理**(Earnshaw's theorem) の結果によれば，電荷を静電ポテンシャルによって 3 次元的に閉じ込めることはできない．したがって，閉じ込めるために 2 つの電極を接地し，他の 2 つを高周波振動電圧で駆動して RF ポテンシャル $\Phi_{\rm rf} = (V_0 \cos\Omega_T t + U_r)[1+(x^2-y^2)/R^2]/2$ を作り出す．ここで $R$ は幾何学的因子である．電極の分割部分は静電容量で結合され，RF ポテンシャルが一定となるように保たれる．$\Psi_{\rm dc}$ と $\Psi_{\rm rf}$ を組み合わせると（$\Omega_T$ に関する）平均で，$x$，$y$，$z$ に関する調和ポテンシャルが作られる．イオンの Coulomb 反発と合わせて，これがトラップ内の $N$ 個のイオンの運動を規定する Hamiltonian を与える：

$$H = \sum_{i=1}^{N} \frac{M}{2}\left(\omega_x^2 x_i^2 + \omega_y^2 y_i^2 + \omega_z^2 z_i^2 + \frac{|\vec{p}_i|^2}{M^2}\right) + \sum_{i=1}^{N}\sum_{j>i} \frac{e^2}{4\pi\epsilon_0|\vec{r}_i - \vec{r}_j|}, \quad (7.92)$$

ここで $M$ は各イオンの質量である．典型的な設計では $\omega_x$，$\omega_y \gg \omega_z$ として，イオンがすべて $\hat{z}$ 軸上に存在するようにする．イオン数が増えるに従ってイオンの幾何学的配置は複雑になりジグザグや他の配列になったりするが，少数イオンが数珠繋ぎ形状でトラップされる簡単な場合に話を限る．

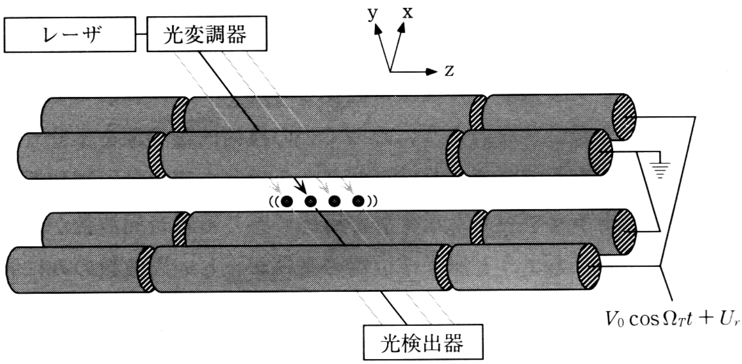



**図 7.7:** イオントラップ量子コンピュータの模式図（縮尺通りではない）．4 電極で作られたポテンシャルの中心にトラップされている 4 個のイオンを示す．通常装置は高真空（$\approx 10^{-8}$ Pa）に保たれ，イオンは近くの高温炉から供給される．変調されたレーザが真空装置の窓を通してイオンを照射し，原子状態の演算と読み出しを行う．

外界との結合が弱くなるとバネに付けた質量が量子システムとして振る舞うように，電位で閉じ込められたイオンの運動も十分に孤立化すると量子化する．最初に量子化が何を意味するかを理解したうえで孤立化の基準を考える．7.3 節で見たように調和振動子のエネルギー準位は $\hbar\omega_z$ の単位で等間隔に分布する．我々が興味を持つイオントラップの領域は，エネルギー固有状態が直線状の一連のイオン**全体**が質量 $MN$ の 1 つの物体となって振動するモードを表す場合である．これを**質量中心**(center of mass) モードと呼ぶ．振動エネルギー $\hbar\omega_z$ の量子を**フォノン**(phonon) と呼び，共振器中の電磁放射の量子を光子と呼ぶように，これも粒子と考える．

上のフォノンによる記述が成立するには，ある基準を満たす必要がある．第 1 に環境との結合が十分小さく，熱的緩和によりシステム状態がランダムにならない（したがって古典的に振る舞う）ことである．近くの変動電界や磁界がイオンに作用して，運動状態がエネルギー固有状態間でランダムに遷移することが物理的に生じ得る．技術的意味で閉じ込め電極を完全な一定電圧源で駆動できないので，このような雑音源はほとんど不可避である．例えば，電圧源は常に有限の内部抵抗を持ち，この抵抗は熱雑音を発生してイオンが感じる時間スケールの変動を起こす．電極の分割部分に加わる電界も変動してイオンの運動をランダムに駆動する．ランダムさが増すとイオンの量子的性質が失われ，その振る舞いは古典

的統計平均で記述したほうが良くなる．例えば，イオンの運動量と位置が明確に定義できるようになるが，これは量子システムでは同時にできないものである．それにもかかわらず実際に多くの実験に必要な時間スケールにおいて，イオンの加熱や位相の乱れを起こさないようにたいていの技術的雑音源を十分うまく制御することができる．ある部分でこれが可能となる重要な理由は，調和振動子近似が成り立つ限り，トラップされたイオンが敏感に感じる雑音周波数が非常に限られているからである．ちょうど原子準位間の遷移が正しい周波数のみに同調した放射で起きるのと同様に，$\omega_z$ の辺りに高いスペクトル電力密度を持つ変動のみがイオンに影響を及ぼす．

イオンが十分冷却されていて，1 次元調和振動近似が成り立つことも重要である．トラップ中心からどの方向にでも大きく変位すれば真のポテンシャルは非放物線的となる．イオンが（一緒に運動するのではなく）互いに相対的に運動する高次の振動モードは，質量中心モードに比べて高いエネルギーを持つ．これが成立してイオンが運動の基底状態に冷却されると，次の高次エネルギー状態への遷移は質量中心フォノンを吸収して起きる．このプロセスは，結晶中の原子で吸収された光子が局部的フォノンを発生することなく結晶全体の反跳を起こす **Mössbauer 効果**(Mössbauer effect) と似ている．

イオンをどのようにして運動の基底準位に冷却するか？ このゴールは $k_{\rm B}T \ll \hbar\omega_z$ を達成することである．ここで $T$ はイオンの運動エネルギーを反映する温度である．これを達成するには本質的に光子が持つのはエネルギーだけではなく，運動量 $p = h/\lambda$ も持つという事実を利用する．ここで $\lambda$ は光の波長である．丁度近づく列車の汽笛が離れる列車より高い音程を持つのと同様に，レーザビームの方向に動く原子は遠ざかる原子よりも少し高いエネルギーの遷移周波数を持つ．レーザが近づく原子だけに吸収されるように周波数を選択すると，光子は逆方向に反跳するので原子は低速化する．この方法を **Doppler 冷却**(Doppler cooling) と呼ぶ．適切に同調した（各軸方向の運動量ベクトル成分を持つ）レーザ光をトラップ原子に照射すると，原子を $k_{\rm B}T \approx \hbar\Gamma/2$ の限界まで冷却できる．ここで $\Gamma$ は冷却に用いる遷移の放射線幅 (radiative linewidth) である．この限界を超えるには図 7.8 に示す**側帯波冷却**(sideband cooling) と呼ぶ別の方法を用いる．これにより $k_{\rm B}T \ll \hbar\omega_z$ の限界に近づくことができる．

もう 1 つ満たさねばならない基準はトラップポテンシャル中のイオン振動の幅が

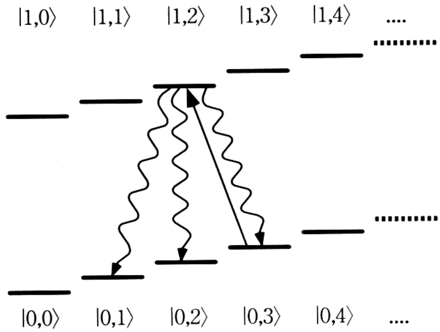



**図 7.8:** $|0,n\rangle$ と $|1,m\rangle$ の間の遷移を示す側帯波冷却法の説明．ここで 0 と 1 は 2 つの電子エネルギー準位，$n$ と $m$ はイオンの運動状態を示すフォノン準位である．レーザ光を電子遷移より 1 フォノン分小さいエネルギーに同調し，例えば図にあるように $|0,3\rangle$ から $|1,2\rangle$ への遷移を起こす（実線矢印）．次に原子はもとの 0 エネルギー状態に減衰し，$|0,1\rangle$，$|0,2\rangle$，$|0,3\rangle$ のいずれかに（ほぼ等確率で）ランダムに遷移する（波線矢印）．実際にはレーザ光が同じエネルギーを有する $|0,n\rangle$ から $|0,n-1\rangle$ へのすべての可能な遷移を起こすことに注意する．しかし $|0,0\rangle$ 状態はこのプロセスに関与せず，究極的にはすべての原子がこの状態に集まる．

入射光の波長に比べて小さいことである．この **Lamb-Dicke の基準** (Lamb-Dicke criterion) は **Lamb-Dicke のパラメータ**(Lamb-Dicke parameter) $\eta \equiv 2\pi z_0/\lambda$ によって表現するのが便利である．ここで $\lambda$ は波長，$z_0 = \sqrt{\hbar/2NM\omega}$ はトラップ内のイオン間隔に対する特徴的長さの尺度である．Lamb-Dicke の基準は $\eta \ll 1$ で与えられる．イオントラップを量子計算に使うには $\eta \ll 1$ である必要はないが，異なるレーザビームが個別イオンを区別できて，論理演算を行うための運動状態の光励起が難しくなりすぎないためには，少なくとも $\eta \approx 1$ であることが望ましい．

### 原子構造

上述のトラップ装置の目的は，計算に適した初期状態であるゼロフォノン状態 ($|0\rangle$) に十分近い振動状態になるように，イオンを冷却することである．同様に量子情報を蓄積できるように，イオンの内部状態を適切に初期化しなければならない．ここではこれらの初期状態とは何かを考え，コヒーレント寿命を推定して，なぜこれが良い q ビット表現なのかを理解する．

我々が考えるトラップイオンの内部状態は，電子スピン $S$ と核スピン $I$ の結合 $F = S + I$ から生じる．これを記述する — **角運動量の和**と呼ぶ — 形式的理論は原子構造を理解するための重要な物理を記述するだけでなく，量子情報にも興味ある機構でもある．7.5.1 項で見たように，原子と相互作用する単一光子は1ユニットの角運動量を与えたり取り去ったりする．しかし原子には軌道角運動量，電子スピン，核スピンという多くの角運動量の起源がある．その起源の一部は光子のエネルギーが選択するエネルギー準位によって決まる．しかし光子はそれ以上の異なる起源を区別することができず，何が起きるかを記述するには，**全**角運動量が一意に定義された原子の性質となる基底を選ばなければならない．

例えば2つのスピン1/2のスピンを考える．この2つのqビット空間に対する「計算」基底は $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$ であるが，状態空間を張るには次の基底を選んでも同様にうまくいく：

$$|0,\ 0\rangle_J = \frac{|01\rangle - |10\rangle}{\sqrt{2}} \tag{7.93}$$

$$|1,\ -1\rangle_J = |00\rangle \tag{7.94}$$

$$|1,\ 0\rangle_J = \frac{|01\rangle + |10\rangle}{\sqrt{2}} \tag{7.95}$$

$$|1,\ 1\rangle_J = |11\rangle. \tag{7.96}$$

これらの基底状態は特別なものである．なぜなら，これらは $j_x = (X_1+X_2)/2$, $j_y = (Y_1 + Y_2)/2$, $j_z = (Z_1 + Z_2)/2$，および

$$J^2 = j_x^2 + j_y^2 + j_z^2 \tag{7.97}$$

で定義される全運動量オペレータの固有状態である．状態 $|j, m_j\rangle_J$ は固有値 $j(j+1)$ を有する $J^2$ の固有状態であると同時に，固有値 $m_j$ を有する $j_z$ の固有状態である．これらの状態は多くの物理的相互作用により自然に選ばれた状態である．例えば $\hat{z}$ 方向の磁界の中で，Hamiltonian $\mu B_z$ 中の磁気モーメント $\mu$ は $\hat{z}$ 方向の全角運動量成分 $m_j$ に比例する．

角運動量の和に関する理論は精巧で十分研究されており，ここでその一端に触れたに過ぎない（興味を持つ読者のために関連する演習を下に示し，章末の「歴史と参考資料」欄に文献の指針を示す）．それにもかかわらず上の例には量子情報に関する興味ある見方がすでに示されている．普通我々は Bell 状態（1.3.6 項：

第 I 巻）のようなもつれ状態は奇妙で非局所的性質を持つので，物質の不自然な状態であると考えがちである．しかし状態 $|0,0\rangle_J$ は Bell 状態である！ なぜ自然界はこのような状態を好むのか？ その理由は磁気モーメントを含む相互作用が 2 つのスピンの交換に関して不変であるという**対称性**にある．この対称性は自然界で実際に広く起こっており，もつれ測定や演算を実行するのに潜在的に極めて有用である．

**演習 7.25:** 全角運動量オペレータは $SU(2)$ に対する交換関係，つまり $[j_i,\ j_k] = i\epsilon_{ikl}j_l$ に従うことを示せ．

**演習 7.26:** $|j,\ m_j\rangle_J$ で定義される基底において $4\times 4$ の行列 $J^2$ と $j_z$ を明示的に書くことにより，$|j,\ m_j\rangle_J$ の性質を証明せよ．

**演習 7.27:（3 つのスピン角運動量状態）** スピン 1/2 の 3 つのスピンを組み合わせると $j=1/2$ と $j=3/2$ を有する全角運動量状態を与えることができる．次の状態：

$$|3/2,\ 3/2\rangle = |111\rangle \tag{7.98}$$

$$|3/2,\ 1/2\rangle = \frac{1}{\sqrt{3}}\Big[|011\rangle + |101\rangle + |110\rangle\Big] \tag{7.99}$$

$$|3/2,\ -1/2\rangle = \frac{1}{\sqrt{3}}\Big[|100\rangle + |010\rangle + |001\rangle\Big] \tag{7.100}$$

$$|3/2,\ -3/2\rangle = |000\rangle \tag{7.101}$$

$$|1/2,\ 1/2\rangle_1 = \frac{1}{\sqrt{2}}\Big[-|001\rangle + |100\rangle\Big] \tag{7.102}$$

$$|1/2,\ -1/2\rangle_1 = \frac{1}{\sqrt{2}}\Big[|001\rangle - |011\rangle\Big] \tag{7.103}$$

$$|1/2,\ 1/2\rangle_2 = \frac{1}{\sqrt{6}}\Big[|001\rangle - 2|010\rangle + |100\rangle\Big] \tag{7.104}$$

$$|1/2,\ -1/2\rangle_2 = \frac{1}{\sqrt{6}}\Big[-|110\rangle + 2|101\rangle - |011\rangle\Big] \tag{7.105}$$

が $j_z = (Z_1+Z_2+Z_3)/2$ （$j_x$ と $j_y$ も同様）および $J^2 = j_x^2 + j_y^2 + j_z^2$ に対して，$J^2|j,\ m_j\rangle = j(j+1)|j,\ m_j\rangle$ および $j_z|j,\ m_j\rangle = m_j|j,\ m_j\rangle$ を満たして，空間の基底を形成することを示せ．これらの状態を得るには複雑

な方法があるが，腕力による直接的方法は単に $J^2$ と $j_z$ の $8\times 8$ 行列を同時に対角化する方法である．

**演習 7.28:（超微細構造）** 7.6.4 項でベリリウムイオンについて調べる．Be では関係する核スピン $I=3/2$ と電子スピン $S=1/2$ が結合して $F=2$ または $F=1$ となる．スピン 3/2 の粒子に対して角運動量オペレータは次式で与えられる：

$$i_x = \frac{1}{2}\begin{bmatrix} 0 & \sqrt{3} & 0 & 0 \\ \sqrt{3} & 0 & 2 & 0 \\ 0 & 2 & 0 & \sqrt{3} \\ 0 & 0 & \sqrt{3} & 0 \end{bmatrix}, \tag{7.106}$$

$$i_y = \frac{1}{2}\begin{bmatrix} 0 & i\sqrt{3} & 0 & 0 \\ -i\sqrt{3} & 0 & 2i & 0 \\ 0 & -2i & 0 & i\sqrt{3} \\ 0 & 0 & -i\sqrt{3} & 0 \end{bmatrix}, \tag{7.107}$$

$$i_z = \frac{1}{2}\begin{bmatrix} -3 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 3 \end{bmatrix}. \tag{7.108}$$

(1) $i_x$, $i_y$, $i_z$ が $SU(2)$ の交換関係を満たすことを示せ．

(2) $f_z = i_z\otimes I + I\otimes Z/2$ および同様に $f_x$, $f_y$, ならびに $F^2 = f_x^2 + f_y^2 + f_z^2$ に対する $8\times 8$ 行列表現を与えよ（ここで $I$ は適切な部分空間における単位オペレータを表す）．$f_z$ と $F^2$ を同時に対角化して，$F^2|F,\ m_F\rangle = F(F+1)|F,\ m_F\rangle$ および $f_z|F,\ m_F\rangle = m_F|F,\ m_F\rangle$ となる基底状態 $|F,\ m_F\rangle$ を求めよ．

異なるスピン状態の重ね合せはどれくらい長く存在できるか？ これを制限する**自然放出**(spontaneous emission) と呼ぶプロセスは，原子が光子を放出して励起状態から基底状態へ遷移するときに生じる．これはランダムな時刻に起き，その割合をこれから推定する．原子が自由空間にあって何も擾乱を受けなければ，

自然放出をすることが奇妙に見えるかも知れない．しかし実際にこのプロセスは原子と電磁界が結合する結果非常に自然に起きるものであり，7.5.2 項で述べた Jaynes-Cummings の相互作用で簡単に記述できる：

$$H_I = g(a^\dagger \sigma_- + a\sigma_+), \tag{7.109}$$

以前にこのモデルを用いてレーザ光と原子の相互作用を記述したが，このモデルは光電界が存在しないときの原子の振る舞いも記述する！ 励起状態にある原子が光子を含まない単一モードと結合する状態 $|01\rangle$ を考える（状態は $|$ 電磁界, 原子 $\rangle$ で表記する）．**これは $H_I$ の固有状態ではないので**，時間が経過しても定常状態にならない．実際に起きることは式 (7.77) のユニタリーオペレータで記述され，これから確率 $p_{\rm decay} = |\langle 10|U|01\rangle|^2$ で原子が基底状態に遷移して光子を放出することがわかる．ここで原子・電磁界結合 $g$ の最低次において

$$p_{\rm decay} = g^2 \frac{4\sin^2 \frac{1}{2}(\omega-\omega_0)t}{(\omega-\omega_0)^2}. \tag{7.110}$$

$\omega$ は光子の周波数，$\hbar\omega_0$ は原子の 2 準位間のエネルギー差である．自由空間にある原子は多くの異なるモードと相互作用する．原子の双極子オペレータを $\vec{\mu}$ としてこの式に結合：

$$g^2 = \frac{\omega_0^2}{2\hbar\omega\epsilon_0 c^2} |\langle 0|\vec{\mu}|1\rangle|^2 \tag{7.111}$$

を代入して全光モードについて積分し（演習 7.29），時間で微分すると 1 秒当たりの遷移確率を得る：

$$\gamma_{\rm rad} = \frac{\omega_0^3 |\langle 0|\vec{\mu}|1\rangle|^2}{3\pi\hbar\epsilon_0 c^5}. \tag{7.112}$$

もし Bohr 磁子を $|\langle 0|\vec{\mu}|1\rangle| \approx \mu_{\rm B} \approx 9\times 10^{-24}$J/T で近似し，周波数 $\omega_0/2\pi \approx$ 10 GHz とすれば，$\gamma_{\rm rad} \approx 10^{-15}{\rm sec}^{-1}$ つまり自然放出の割合は 3 000 000 年に 1 回以下となる．この計算は原子状態の推定寿命の代表的値である．超微細状態は理論上極めて長いコヒーレンス時間を有していることがわかる．これは実験で数十秒から数十時間の寿命が観測されているのと矛盾しない．

**演習 7.29:（自然放出）** 自然放出率の式 (7.112) は式 (7.110)，(7.111) より次のステップで導き出せる：

(1) 次式を積分する：

$$\frac{1}{(2\pi c)^2}\frac{8\pi}{3}\int_0^\infty \omega^2 p_{\rm decay}\,d\omega, \tag{7.113}$$

ここで $8\pi/3$ は偏光に関する和と立体角 $d\Omega$ の積分から生じ，$\omega^2/(2\pi c)^3$ は 3 次元空間のモード密度から生じる．（ヒント：積分下限を $-\infty$ に拡張するとよい．）

(2) この結果を $t$ で微分して $\gamma_{\rm rad}$ を求める．

$g^2$ の形は量子電気力学の結果によるものである．これを認めるとここに示す残りの計算は実際に Jaynes-Cummings 相互作用によるものである．ここでも単一原子・単一光子領域の性質を調べると，摂動論によることなく原子の基礎的性質が導かれる！

**演習 7.30:（電子状態の寿命）** $\gamma_{\rm rad}$ に対するのと同じ計算をして電子遷移，つまり $\Delta n \neq 0$ のエネルギー準位変化を伴う遷移に対して期待される寿命が推定ができる．この遷移で原子の電気双極子モーメントが電磁界とが相互作用して結合し

$$g_{\rm ed}^2 = \frac{\omega_0^2}{2\hbar\omega\epsilon_0}|\langle 0|\vec{\mu}_{\rm ed}|1\rangle|^2. \tag{7.114}$$

これから自然放出確率が得られる：

$$\gamma_{\rm rad}^{\rm ed} = \frac{\omega_0^3|\langle 0|\vec{\mu}_{\rm ed}|1\rangle|}{3\pi\hbar\epsilon_0 c^3}. \tag{7.115}$$

$|\langle 0|\vec{\mu}_{\rm ed}|1\rangle| \approx qa_0$, $\omega_0/2\pi \approx 10^{15}$Hz として $\gamma_{\rm rad}^{\rm ed}$ の値を求めよ．ここで $q$ は電荷，$a_0$ は Bohr 半径である．この結果は超微細構造に比べて電子状態が如何に早く遷移し得るかを示す．

### 7.6.2 Hamiltonian

前節で得た調和形電磁トラップと簡単化した原子構造モデルを組み合わせると，イオントラップ量子情報プロセッサの簡単な玩具モデル (toy model) が得られる．単一の 2 準位スピンが通常の磁気双極子相互作用 $H_I = -\vec{\mu}\cdot\vec{B}$ を通じて電磁界と相互作用をすると考える．ここで双極子モーメント $\vec{\mu} = \mu_m\vec{S}$ はスピンオペレー

タ $S$ に比例し，磁界 $\vec{B} = B_1 \hat{x} \cos(kz - \omega t + \varphi)$，$B_1$ は磁界強度，$k$ はその $\hat{z}$ 方向の運動量，$\omega$ は周波数，$\varphi$ は位相である．本節ではスピンオペレータとして $S_x = X/2,\ S_y = Y/2,\ S_z = Z/2$ を使用する．これらは Pauli のオペレータと因子 2 だけ異なる．

通常の電磁界相互作用に加えて振動モードとの相互作用も存在する．スピンはエネルギースケール $\hbar\omega$ の調和ポテンシャル内に物理的に閉じ込められ（図 7.9），その位置が**量子化**されてそれをオペレータで $z = z_0(a^\dagger + a)$ と書かねばならない．ここで $a^\dagger$ と $a$ は粒子の振動モードに対する上昇・下降オペレータでありフォノンの生成・消滅を表現する．

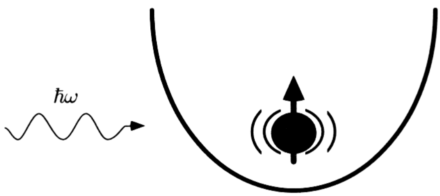



**図 7.9:** トラップされたイオンの玩具モデル．2 つの内部状態を有し電磁放射と相互作用する調和ポテンシャル中の粒子．

粒子が最低次の振動モード近くまで冷却され，ポテンシャル井戸中の振動幅が入射光の波長より小さい，つまり Lamb-Dicke のパラメータ $\eta \equiv kz_0$ が小さいと仮定する．スピンの Rabi 周波数を $\Omega = \mu_m B_1/2\hbar$ で定義し，$S_x = (S_+ + S_-)/2$ を思い出すと $\eta$ が小さい極限で相互作用 Hamiltonian は簡単になって：

$$H_I = -\vec{\mu} \cdot \vec{B} \tag{7.116}$$

$$\approx \left[\frac{\hbar\Omega}{2}\left(S_+ e^{i(\varphi-\omega t)} + S_- e^{-i(\varphi-\omega t)}\right)\right] + \left[i\frac{\eta\hbar\Omega}{2}\left\{S_+ a + S_- a^\dagger + S_+ a^\dagger + S_- a\right\}\left(e^{i(\varphi-\omega t)} - e^{-i(\varphi-\omega t)}\right)\right]. \tag{7.117}$$

第 1 項の括弧は 7.5.2 項で見たように通常の Jaynes-Cummings の Hamiltonian から生じ，スピンの場所 $z$ が一定のときに起きるものである．しかし $B_1$ が強いコヒーレント状態である限りその量子的性質は無視できて，内部原子状態の時間発展を記述する Hamiltonian だけを扱えばよいので，この項は簡単化されて光子

オペレータを含まない．実際電界のコヒーレント状態が原子と相互作用をした後で（十分良い近似で）もつれ状態にならないのは注目すべきことである．これは深い意味を持っており，本章の最後の問題 7.3 でさらに探求する．また 7.7.2 項で共振について述べる際にもこれについて触れる．

第 2 項の括弧はイオンから見える磁界が位置に依存することにより生じる，イオンの運動状態とスピン状態の結合を記述している．中括弧中の 4 項は 4 つの遷移（2 つは上向き，2 つは下向き）に相当し，図 7.10 に示されるように赤色シフトと青色シフトの運動側帯波と呼ぶ．

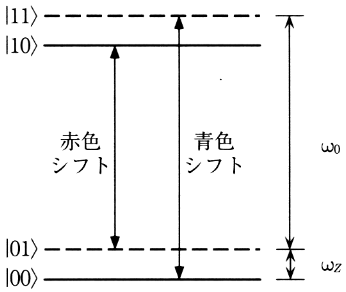



**図 7.10:** トラップイオンの玩具モデルのエネルギー準位．単一フォノンの生成と消滅に対応した赤色シフトと青色シフトの運動側帯波遷移を示す．この他に無限に続く運動状態が存在するが通常は関与しない．状態は $|n, m\rangle$ を記述し，$n$ はスピン状態，$m$ はフォノンの数を表す．

この側帯波遷移が周波数 $\omega_0 \pm \omega_z$ を持つ理由は，自由粒子 Hamiltonian を含めると容易に理解できる．

$$H_0 = \hbar\omega_0 S_z + \hbar\omega_z a^\dagger a, \tag{7.118}$$

これによりスピンとフォノンは次の時間発展をする：

$$S_+(t) = S_+ e^{i\omega_0 t} \qquad S_-(t) = S_- e^{-i\omega_0 t} \tag{7.119}$$

$$a^\dagger(t) = a^\dagger e^{i\omega_z t} \qquad a(t) = a e^{-i\omega_z t}. \tag{7.120}$$

したがって，$H_0$ の参照フレームでの $H_I' = e^{iH_0 t/\hbar} H_I e^{-iH_0 t/\hbar}$ の主要項は：

$$H_I' = \begin{cases} i\frac{\eta\hbar\Omega}{2}(S_+ a^\dagger e^{i\varphi} - S_- a e^{-i\varphi}), & \omega = \omega_0 + \omega_z \\ i\frac{\eta\hbar\Omega}{2}(S_+ a e^{i\varphi} - S_- a^\dagger e^{-i\varphi}), & \omega = \omega_0 - \omega_z \end{cases} \tag{7.121}$$

ここで電磁波の周波数 $\omega$ を右側に示した.

$N$ 個のスピンが単一の質量中心振動モードに属し，そのエネルギーがシステムのどの振動モードよりもはるかに低いならば，上のモデルをスピン 1 個から同じ調和ポテンシャルに閉じ込められたスピン $N$ 個に拡大するのは容易である．この理論を直接拡張するときに必要な変更は，$N$ 個すべてが集団で動くので $\Omega$ を $\Omega/\sqrt{N}$ 置き換えるだけでよい.

### 7.6.3 量子計算

トラップイオンを用いた量子計算には原子の初期状態に施す任意のユニタリー変換を構築する必要がある．これを如何に行うかを 3 段階で説明しよう.

(1) 原子の内部状態（スピン）に対して任意の単一 q ビット演算を行う方法.

(2) スピン状態とフォノン状態間の 2 - q ビット制御ゲートを実行する方法.

(3) スピンとフォノン間で量子情報を入れ換える方法.

これらの構成要素を準備した後に，状態生成と読み出し機能を備えた制御 NOT ゲートの実験について述べる.

**単一 q ビット演算**

周波数 $\omega_0$ に同調した電磁波を加えると内部 Hamiltonian の項は：

$$H_I^{\text{internal}} = \frac{\hbar\Omega}{2}\left(S_+ e^{i\varphi} + S_- e^{-i\varphi}\right). \tag{7.122}$$

$\varphi$ と相互作用時間を適切に選ぶと，回転演算 $R_x(\theta) = \exp(-i\theta S_x)$ と $R_y(\theta) = \exp(-i\theta S_y)$ の実行が可能になる．定理 4.1 によればこれを使ってスピン状態に対して任意の単一 q ビット演算ができる．$j$ 番目のイオンの回転を，例えば $R_{xj}(\theta)$ のように下添字で表記する.

**演習 7.31:** 回転 $R_y$ と $R_x$ から Hadamard ゲートを構築せよ.

### 制御位相反転ゲート

1 個の q ビットが原子の内部スピン状態に蓄積され，もう 1 つの q ビットが $|0\rangle$ と $|1\rangle$ のフォノン状態に蓄積されると想定する．この場合，次のユニタリー変換により制御位相反転ゲートが実行できる．

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}. \tag{7.123}$$

これは図 7.11 に示す第 3 のエネルギー準位を持つ原子で容易に説明できる（基本的にはこの付加的な準位は必要ない．問題 7.4 参照）．レーザを周波数 $\omega_{\rm aux}+\omega_z$ に同調して状態 $|20\rangle$ と $|11\rangle$ 間で遷移を起こす．これを起こす Hamiltonian は：

$$H_{\rm aux} = i\frac{\eta\hbar\Omega'}{2}\left(S'_+e^{i\varphi} + S'_-e^{-i\varphi}\right), \tag{7.124}$$

ここで $S'_+$ と $S'_-$ は状態 $|20\rangle$ と $|11\rangle$ 間の遷移を表し，高次の運動状態は励起されていないと仮定する．この周波数は一義的に決まるので，他の遷移は励起されないことに注意する．$2\pi$ パルスとなるように位相と時間幅を調整したレーザ光を照射する，つまりこれは状態 $|11\rangle$ と $|20\rangle$ で張られた空間で回転 $R_x(2\pi)$ を起こすもので，ユニタリー変換 $|11\rangle \to -|11\rangle$ に他ならない．$|1,\ 2\rangle$ のように希望しない準位は確率振幅がゼロなので，他の状態はすべて変化しない．これで希望通り式 (7.123) の変換が実現される．このゲートを $C_j(Z)$ と書く（これは制御 $Z$ ゲート演算を表す）．ここで $j$ はゲートを適用するイオンの番号を表す．質量中心フォノンなので全イオンが同じフォノンを共有しており，このため論文では技術者の言葉でフォノン「バス」(phonon bus) q ビットと呼ばれている．

### 交換ゲート

最後に原子の内部スピン状態とフォノン状態間で q ビットの交換を実行する方法が必要である．これを行うにはレーザ周波数を $\omega_0-\omega_z$ に同調し，$|01\rangle$ と $|10\rangle$ が張る部分空間で回転 $R_y(\pi)$ を行うように位相を調整する．これは $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$

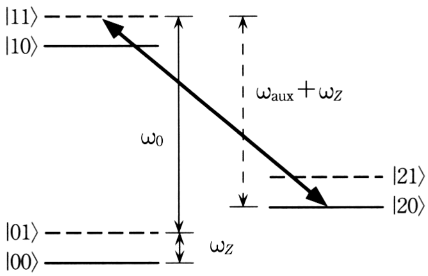



**図 7.11:** イオントラップ中の 3 準位原子のエネルギー準位．各準位が 2 つのフォノン状態を持つ．ラベル $|n,\ m\rangle$ は原子の状態 $n$ とフォノンの状態 $m$ を示す．制御位相反転ゲートを実行するのに遷移 $|20\rangle \leftrightarrow |11\rangle$ を使用する．

空間でのユニタリー変換になる：

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}. \tag{7.125}$$

もし初期状態が $a|00\rangle + b|10\rangle$（つまりフォノンが最初は $|0\rangle$ にある）ならば，交換後の状態は $a|00\rangle + |01\rangle$ となり望む交換演算が実行される．イオン $j$ に働くときにこれを $\mathrm{SWAP}_j$ と書く．逆演算 $\overline{\mathrm{SWAP}}_j$ は $R_y(-\pi)$ に対応する．技術的には $R_y(\pi)$ の $|10\rangle\langle 01|$ 要素に負号があるので完全な交換ではないが，相対位相を別としてそれと等価である（演習 4.26 参照）．したがって，交換の代わりに「写像演算」(mapping operation) と呼ぶことがある．

### 制御 NOT ゲート

これらのゲートを集めると，次の一連の演算によって $j$ 番目のイオン（制御）と $k$ 番目のイオン（標的）に働く制御 NOT ゲートが構築できる：

$$\mathrm{CNOT}_{jk} = H_k\ \overline{\mathrm{SWAP}}_k\ C_j(Z)\ \mathrm{SWAP}_k\ H_k, \tag{7.126}$$

（通常の行列演算と同様に時間は右から左へ経過する．）ここで $H_k$ は Hadamard ゲート（イオン $k$ に及ぼす回転 $R_y$ と $R_x$ から構成）である．これは式 (7.46) と

同様にビームスプリッタと Kerr 媒質を使って制御 NOT ゲートが構成できるのと似ている．

### 7.6.4　実　験

トラップされた単一イオンを用いて制御 NOT ゲートの実験が行われており（章末の「歴史と参考資料」参照），その方法はまさに見識に満ちたものである．実験では $^9Be^+$ イオン 1 個が同軸 RF 共振器イオントラップに捕獲される．このトラップは図 7.7 の直線状イオントラップと異なる幾何学的配置であるが同じ機能を持ち，実際のイオントラップを図 7.12 に示す．ベリリウムを選んだ理由は図 7.13 に示すように便利な超微細準位と電子準位を持っているからである．$^2S_{1/2}(1,\ 1)$ と $^2S_{1/2}(2,\ 2)$ のエネルギー準位（演習 7.28）を原子の内部 q ビット状態として使用し，$|0\rangle$ と $|1\rangle$ のフォノン状態をもう 1 つの q ビット（図中の $n=1, n=2$ で表示）

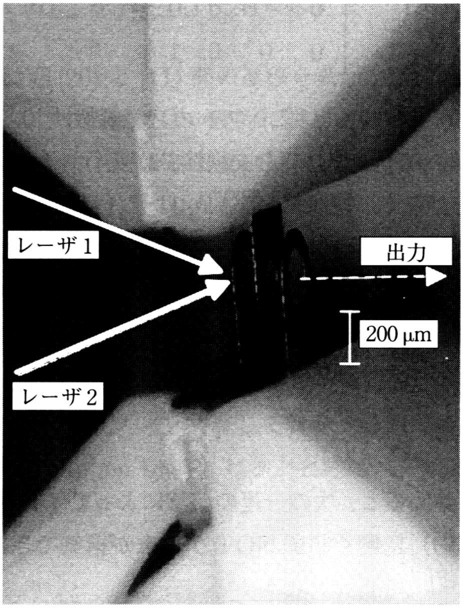



**図 7.12:** イオンを閉じ込めるために微細加工で作られた楕円電極イオントラップの写真．このトラップに捕獲されるイオンはベリリウムでなくバリウムであるが，基本原理は本文で述べたのと同じである．IBM Almaden 研究センタの R. DeVoe と C. Kurtsiefer の厚意による．

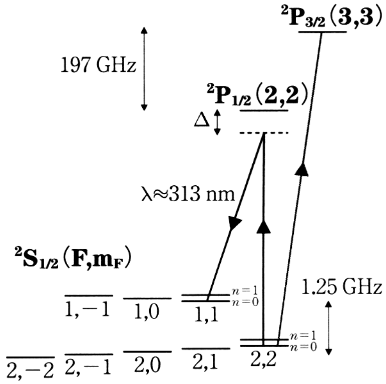



**図 7.13:** イオントラップ実験に用いられた $^9Be^+$ のエネルギー準位．NIST の C. Monroe の厚意による．

として用いる．$^2S_{1/2}(1,\ 1)$ と $^2S_{1/2}(2,\ 2)$ 準位間の $\sim 313$ nm の遷移は，単一のレーザ波長を同調するのではなく，2 つのレーザの差周波数を同調することにより起こさせる．この **Raman 遷移**(Raman transition) 法はレーザ位相の安定性への要求を楽にする．$^2S_{1/2}$ 状態はシステムに加えられた 0.18 ミリテスラの磁界により異なるエネルギーを有しており，$^2S_{1/2}(2,\ 0)$ 状態を補助状態として用いる．トラップイオンはトラップ中で $(\omega_x,\ \omega_y,\ \omega_z)/2\pi = (11.2,\ 18.2,\ 29.8)$MHz の振動周波数を有し，基底状態 $n_x = 0$ の波動関数の広がりは約 7nm なので Lamb-Dicke のパラメータは $\eta_x = 0.2$ となる．共鳴遷移の Rabi 周波数は $\Omega/2\pi = 140$ kHz，2 つの運動側帯波は $\eta_x\Omega/2\pi = 30$ kHz，補助遷移は $\eta_x\Omega'/2\pi = 12$ kHz である．

Doppler 冷却と側帯波冷却を用いてイオン状態を初期化する．約 95 % の確率で状態 $|00\rangle = |^2S_{1/2}(2,\ 2)\rangle\ |n_x = 0\rangle$ が得られる．次に単一 q ビット演算を使ってイオンの内部および運動状態を 4 つの基底状態 $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$ の 1 つに準備し，次に 3 つのパルスを用いて制御 NOT を実行する．これにより内部状態 q ビットに回転 $R_y(\pi/2)$ を施し，2 つの q ビット間で制御 NOT を実行し，最後に内部状態 q ビットに回転 $R_y(-\pi/2)$ を実行する．図 7.14 に描いたこの回路が制御 NOT 演算を実行することを示すのは簡単である（演習 7.32）．

計算結果の読み出しは 2 回の測定により行う．最初に「循環」遷移 $^2S_{1/2}(2,\ 2)-{}^2P_{3/2}(3,\ 3)$ に同調した右回り円偏光（+）を照射したときにイオンが発する蛍光を測定する．この光は $^2S_{1/2}(1,\ 1)$ 状態とあまり結合せず，したがって測定した

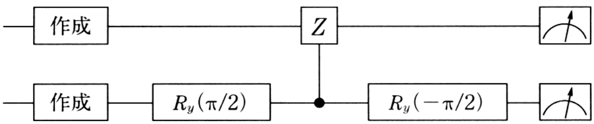



**図 7.14:** イオントラップの制御 NOT の量子回路モデル．上の配線はフォノン状態，下はイオンの内部超微細状態を示す．

蛍光強度は内部状態 q ビットが状態 $|0\rangle$ にある確率に比例する．これは射影測定である．この遷移は — 光子を吸収したイオンが $^2P_{3/2}(3,\ 3)$ 状態に励起し，光子を放出して出発点の $^2S_{1/2}(2,\ 2)$ 状態に戻る — サイクルを何回も繰り返すので，強力な測定法となる．数千回以上のサイクルの繰り返しが可能なので良好な統計が累積される．第 2 の測定は最初の測定に似ているがはじめに交換パルスを加えて，運動状態と内部状態の q ビットを入れ換える．これにより運動状態の q ビットを射影測定する．

実際に行われた実験で制御 NOT 演算の古典的な真理値表が実証され，重ね合せ入力状態を準備して出力密度行列を測定することにより，プロセストモグラフィー（8 章：第 III 巻）で原理上ユニタリー変換の性質が完全に解明されている．実験に用いた光強度で制御 NOT 演算を行うのに約 50 マイクロ秒を要する．一方，測定されたコヒーレンス時間は数百～数千マイクロ秒である．主要なコヒーレンス劣化要因にはレーザビーム強度，RF イオントラップの駆動周波数と電圧，外部磁場の不安定性がある．さらに実験ではたった 1 個のイオンと 2 個の q ビットしか含まれておらず計算には不十分である．実用には制御 NOT が 1 つのイオンと運動状態の間だけでなく一般に異なるイオン間にも適用できなければならない．

しかし技術的な制約はいずれ克服され，短寿命の運動状態を断続的に用いて内部原子状態の長いコヒーレンス時間を利用することにより，寿命の問題は解決できるであろう．多数イオンへの拡張も概念上可能である．図 7.15 に 40 個の水銀



**図 7.15:** 約 40 個のトラップされた水銀（$^{199}Hg^+$）原子イオンの蛍光像．イオン間隔は約 15$\mu$m，2 つの大きなギャップはプローブレーザに応答しない水銀の同位元素による．NIST の D. Wineland の厚意により掲載．

イオンの列がトラップされた様子を示す．このようなシステムを有用な量子情報処理機械として働かせるにはまだ多くの障害があるが，技術的驚きはいつも終わりのない物語である．何時の日かこのようなトラップされたイオンが多分量子コンピュータのレジスタになるであろう．

**演習 7.32:** 図 7.14 の回路がフォノン状態を制御 q ビットとした制御 NOT 回路と（相対位相を除いて）等価であることを示せ．

### 7.6.5 イオントラップ量子コンピュータ

- **q ビット表現：** 原子の超微細状態（核スピン）とトラップされた原子の最低次振動モード（フォノン）．
- **ユニタリー時間発展：** レーザパルス照射により，Jaynes-Cummings の相互作用を通じて，原子状態を外部から操作して任意の変換を構築できる．q ビットは共有フォノンを通じて相互作用をする．
- **初期状態の生成：** （トラップと光ポンピングにより）原子を運動の基底状態と超微細基底状態まで冷却する．
- **読み出し：** 超微細状態の分布を測定する．
- **欠点：** フォノン寿命が短く，イオンを運動の基底状態に準備するのが難しい．

## 7.7 核磁気共鳴

もしもスピン・スピン結合だけを大きくできて，制御ができるならば核スピンシステムは量子計算にとってほぼ理想的であろう．これは前節におけるイオントラップの研究から得た重要な知見である．イオントラップ量子コンピュータの主な欠点は光子が仲介するスピン・スピン結合が弱く，コヒーレンス劣化を受け易いことである．この限界を克服する 1 つの方法は単一原子の代わりに分子を閉じ込めることである — 磁気双極子と電子が仲介する隣接原子核間の Fermi 接触相互作用 (Fermi contact interaction) ならば強い自然な結合が得られるであろう．しかし，振動モードが多いために単一分子を閉じ込めて冷却するのが困難であり，

したがってトラップ分子の核スピンを光学的に操作し検出することは，特別な場合を除いて容易でなかった．

他方でRF帯の電磁波を用いて核スピンを直接操作し検出することは核磁気共鳴（NMR）として非常に発達している分野である．この技術は化学において広く用いられ，例えば液体・固体・ガスの性質を調べて分子構造を決定したり，生物システムにまで至る材料の画像化をすることができる．これらの多くの応用によってNMRの技術は極めて高性能になり，1回の実験で数百・数千種類にも及ぶ原子核を制御し観測することができる．

しかしNMRを量子計算に用いるには問題が2つある．1つは核磁気モーメントが小さいために，測定可能な誘導信号を得るためには多数（$\approx 10^8$ 以上）の分子が存在しなければならない．理論上単一分子ならば立派な量子コンピュータになるであろうが，分子のアンサンブルの場合にはどうであろうか？ 特にNMR測定の出力は全分子の信号の**平均値**であり，量子コンピュータにおいてアンサンブルの平均出力が意味を持ち得るであろうか？ 第2に通常NMRは室温で熱平衡にある物理システムに対して適用され，スピンエネルギー $\hbar\omega$ は $k_B T$ に比べて十分小さい．これはスピンの初期状態がほとんど完全にランダムであることを意味する．従来の量子計算ではシステムを純粋状態に準備する必要があるが，どのようにして高いエントロピーの混合状態にあるシステムで量子計算を実行できるのであろうか？

通常システムの熱的性質から生じる厳しい制約はあるものの，これら2つの問題が解決されて，NMRは量子計算を実行できる非常に魅力的で見通しの良い方法となった．このNMRから多くのことを学ぶことができる：例えば現実的Hamiltonianを制御して任意のユニタリー変換を行うテクニック，コヒーレンス劣化（と系統的誤り）の性質を明らかにして克服する方法，全システムに完全な量子アルゴリズムを実装する際に部品構成上考慮すべき事項等である．最初に物理的装置とそれに含まれる主要なHamiltonianについて述べる．次に熱的な入力状態やアンサンブルの問題があるにもかかわらず，如何にしてNMRを用いる量子情報処理が可能になるのかを議論し，最後に量子アルゴリズムの実行を実証した実験とこの方法の欠点について述べる．

### 7.7.1 物理的装置

最初に装置の概要について述べて，後でその働きを数式的にモデル化する．ここで注目する液体試料用のパルス NMR システムは 2 つの主要部分，つまり試料と NMR 分光器から成っている．使用できる典型的な分子はスピン 1/2 を持つ $n$ 個の陽子（つまり水素原子核）を含んでおり（この他にスピン 1/2 を持ち，利用できる原子核には $^{13}$C，$^{19}$F，$^{15}$N および $^{31}$P がある），約 11.7 テスラの磁界中に置くと約 500 MHz の信号を出す．分子内の異なる原子核の周波数は，化学的環境の遮蔽効果によって局所的磁界が異なるために，数十～数百 kHz だけ異なる．分子は通常溶液に溶解し，分子間相互作用が無視できるまで濃度を希釈しており，$n$ 個の q ビットによる量子「コンピュータ」のアンサンブルとしてシステムを記述できる．

分光器それ自体は RF 電子回路と巨大な超伝導磁石で構成し，図 7.16 に示すように磁石の間隙内にガラス管に収めた試料を置く．$\hat{z}$ 方向の静磁界 $B_0$ は 1 cm 当たり $10^9$ 分の 1 以下の一様さに調整されている．横方向平面内の直交する鞍部状 Helmholtz コイルが $\hat{x}$ と $\hat{y}$ 方向に小さな振動磁界を発生する．これらの磁界をパルスで素早くオン・オフして，核磁気状態を操作する．同じコイルを同調回路の一部にして（回転磁石が近くのコイルに交流電流を誘起するのと同じように）歳差運動をする原子核が発生する RF 信号をピックアップする．

典型的な実験では，最初に原子核が熱平衡に達するまで長時間待機する．これ

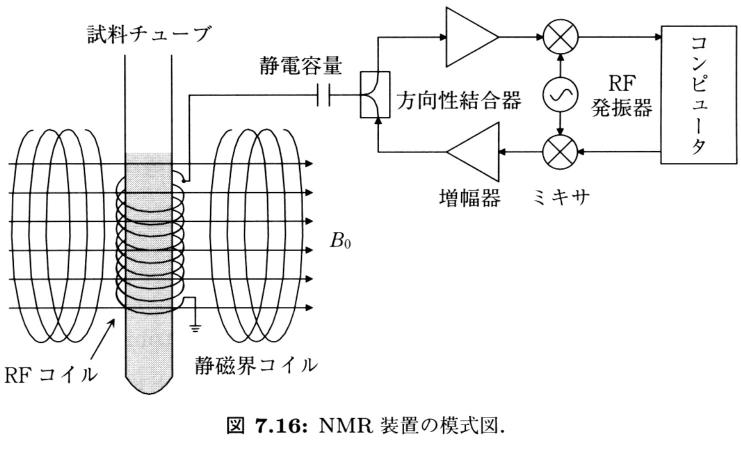



**図 7.16:** NMR 装置の模式図．

にはよく調製された試料で数分を要する．次に（古典）コンピュータの制御に従って，原子核スピンの状態が所望の変換を起こすように RF パルスを加える．高出力パルス増幅器のスイッチを切って高感度前置増幅器を動作させ，スピンの最終状態を測定する．**自由誘導減衰**(free induction decay) と呼ぶこの出力を周波数スペクトルに Fourier 変換すると，そのピークの面積がスピン状態の関数となる (図 7.17)．

観測量を不完全にする要因となり得る重要な事項が沢山ある．例えば静磁界に空間的不均一性があると，磁界の異なる部分にある原子核が異なる周波数で歳差運動を行い，スペクトル線幅が広がる．もっと難しい問題は磁界 $B_0$ と垂直に配置されるコイルによって作られる RF 磁界の不均一性である．この幾何学的配置の制約と $B_0$ の均一性に対する厳しい要請のために，RF 磁界が不均一でコイルが小さくなり原子核システムの制御が不完全になる．またパルスのタイミング，電力の安定性，位相，周波数も重要な要素であるが，イオントラップと異なり周波数が低いのでこれらのパラメータは制御し易い．システムの基本的な数式的記述と NMR を使った量子情報処理の実行手法を理解したうえで，7.7.4 項でこれら不完全性に関してもう一度取り扱う．

### 7.7.2　Hamiltonian

NMR の基礎理論はここで述べるスピン 1 個および 2 個の理想的モデルにより理解できる．最初のステップで電磁界放射と単一の磁気スピンの相互作用を記述する．次に分子内に発生するスピン間結合の物理的性質を考える．これらのツールにより，熱平衡状態の初期状態を変換して生じる，磁化を読み出すモデルを作ることができる．最後にコヒーレンス劣化の現象論的モデルと，そのパラメータ $T_1$，$T_2$ を実験で定める方法を述べる．

#### 単一スピンの運動

古典的電磁界と 2 準位スピンの磁気的相互作用は Hamiltonian $H = -\vec{\mu} \cdot \vec{B}$ で記述できる．ここで $\vec{\mu}$ はスピン，$\vec{B} = B_0\hat{z} + B_1(\hat{x}\cos\omega t + \hat{y}\sin\omega t)$ は典型的な印加磁界である．$B_0$ は非常に大きな静磁界であり，時間変化をする $B_1$ は通常 $B_0$

より数桁小さい強度なので，従来このシステムを調べるのに摂動論が用いられてきた．しかし 2 章の Pauli の行列の方法を用いると，このシステムの Schrödinger 方程式は摂動論なしで直接解くことができる．Hamiltonian を Pauli の行列で書くと：

$$H = \frac{\omega_0}{2} Z + g(X \cos \omega t + Y \sin \omega t), \tag{7.127}$$

ここで $g$ は磁界の強度 $B_1$ に，$\omega_0$ は $B_0$ にそれぞれ関係し，$X$, $Y$, $Z$ はいつもの通り Pauli の行列である．$|\varphi(t)\rangle = e^{i\omega t Z/2}|\chi(t)\rangle$ を定義して，Schrödinger の方程式：

$$i\partial_t|\chi(t)\rangle = H|\chi(t)\rangle \tag{7.128}$$

を次のように書き換える：

$$i\partial_t|\varphi(t)\rangle = \left[e^{i\omega Zt/2} H e^{-i\omega Zt/2} - \frac{\omega}{2} Z\right] |\varphi(t)\rangle. \tag{7.129}$$

ここで

$$e^{i\omega Zt/2} X e^{-i\omega Zt/2} = (X \cos \omega t - Y \sin \omega t), \tag{7.130}$$

なので式 (7.129) は簡単化されて次式となる：

$$i\partial_t|\varphi(t)\rangle = \left[\frac{\omega_0 - \omega}{2} Z + gX\right] |\varphi(t)\rangle. \tag{7.131}$$

ここで右辺の状態の前の因子は実効的に「回転フレーム」(rotating frame) の Hamiltonian と見なすことができて，この方程式の解は：

$$|\varphi(t)\rangle = e^{i\left[\frac{\omega_0 - \omega}{2} Z + gX\right]t} \, |\varphi(0)\rangle. \tag{7.132}$$

この解の振る舞いから共鳴の概念が導ける．式 (4.8) を用いるとこの解は回転軸：

$$\hat{n} = \frac{\hat{z} + \frac{2g}{\omega_0 - \omega}\hat{x}}{\sqrt{1 + \left(\frac{2g}{\omega_0 - \omega}\right)^2}} \tag{7.133}$$

の回りで回転角：

$$|\vec{n}| = t\sqrt{\left(\frac{\omega_0 - \omega}{2}\right)^2 + g^2} \tag{7.134}$$

だけ回転する q ビットの回転であると理解できる．$\omega$ が $\omega_0$ から遠く隔たっているときは，スピンが磁界 $B_1$ から受ける影響は無視できる．スピンの回転軸は $\hat{z}$ にほぼ平行であり，その時間発展は自由な $B_0$ Hamiltonian によるものとほぼ正確に一致するからである．他方 $\omega_0 \approx \omega$ のときには $B_0$ の寄与が無視できて，$\hat{x}$ 軸の回りの回転に対応して小さな磁界 $B_1$ が状態に大きな変化をもたらす．適切な周波数に同調したときに，小さな摂動がスピンシステムに大きな効果をもたらすことが，核磁気共鳴における「共鳴」の原因である．もちろん同じ効果が，7.5.1 項で（説明なく）示した，特別に同調したレーザ電界に対して 2 準位原子が有する選択性の核心でもあった．

一般に $\omega = \omega_0$ のときに，単一スピンの回転フレーム Hamiltonian は次のように書ける：

$$H = g_1(t)X + g_2(t)Y, \tag{7.135}$$

ここで $g_1, g_2$ は加えられた横方向 RF 磁界の強度の関数である．

**演習 7.33:（磁気共鳴）**　式 (7.128) を簡単化すると式 (7.129) になることを示せ．どのような実験室フレーム Hamiltonian から回転フレーム Hamiltonian (7.135) が導かれるか？

**演習 7.34:（NMR 周波数）**　核 Bohr 磁子を用いて 11.8 テスラの磁界中の陽子の歳差周波数を求めよ．10 マイクロ秒で 90° 回転されるには磁界 $B_1$ は何ガウスでなければならないか？

### スピン・スピン結合

対象とするシステムには通常 1 個以上のスピンが存在する．$^1$H, $^{13}$C, $^{19}$F, $^{15}$N はすべて核スピン 1/2 を持っている．これらのスピンは 2 つの主要な機構を通じて相互作用をする：つまり直接的な双極子結合と，化学結合を通じて電子が仲介する間接的相互作用である．空間を通じた双極子結合は次の形の相互作用 Hamiltonian で記述される：

$$H^{\mathrm{D}}_{1,2} = \frac{\gamma_1\gamma_2\hbar}{4r^3}\big[\vec{\sigma}_1 \cdot \vec{\sigma}_2 - 3(\vec{\sigma}_1 \cdot \hat{n})(\vec{\sigma}_2 \cdot \hat{n})\big], \tag{7.136}$$

ここで $\hat{n}$ は2つの核を結ぶ方向の単位ベクトル，$\vec{\sigma}$ は磁気モーメントベクトル（の2倍）である．低粘性溶液では双極子相互作用は速やかに平均化される．これを数学的に計算するには，双極子結合エネルギーのスケールに比べて平均化が早くなるに従って，$\hat{n}$ に関する $H^{\mathrm{D}}_{1,2}$ の球面平均がゼロになるのを示せばよい．

化学結合を通じた相互作用は単に「$J$ 結合 ($J$-coupling)」とも呼び，化学結合で共有された電子が仲介する間接的相互作用である．1つの核が見る磁界がそれを取り巻く電子雲の状態により摂動を受け，その電子雲は電子の波動関数と核の重なりを通じて別の核と相互作用をする（Fermi 接触相互作用）．この結合は次の形を有する：

$$H^{J}_{1,2} = \frac{\hbar J}{4}\vec{\sigma}_1 \cdot \vec{\sigma}_2 = \frac{\hbar J}{4} Z_1 Z_2 + \frac{\hbar J}{8}\big[\sigma_+\sigma_- + \sigma_-\sigma_+\big]. \tag{7.137}$$

$J$ が（一般にはテンソルであるが）スカラーの場合を考える．これは結合が弱い場合の溶液や，相互作用をする核種が大きく異なる歳差周波数を有する場合に優れた近似である．この場合は次式で記述できる：

$$H^{J}_{1,2} \approx \frac{\hbar}{4} J Z_1 Z_2. \tag{7.138}$$

**演習 7.35:（運動による狭幅化）** $H^{D}_{1,2}$ を $\vec{n}$ にわたって球面で平均化するとゼロになることを示せ．

### 熱平衡

核磁気共鳴がこれまでに本章で調べた他の物理システムと大きく異なる点は，システムのアンサンブルを用いることと，基本とする測定がアンサンブル平均であることである．さらに初期状態を基底状態のような特別な状態にするために，一般的な方法を用いることができない．実際のところこれを行うのは現在の技術で困難な課題である．

これに代わって初期状態は次の熱平衡状態である：

$$\rho = \frac{e^{-\beta H}}{\mathcal{Z}}, \tag{7.139}$$

ここで $\beta = 1/k_{\mathrm{B}}T$，$\mathcal{Z} = \mathrm{tr}\ e^{-\beta H}$ は通常の分配関数の正規化係数であって，これにより $\mathrm{tr}(\rho) = 1$ が保証される．室温で典型的な原子核において，通常の磁界

で $\beta \approx 10^{-4}$ なので，$n$ 個のスピンシステムに対して次の高温近似が当てはまる：

$$\rho \approx 2^{-n}\big[1-\beta H\big]. \tag{7.140}$$

スピン・スピン相互作用は歳差周波数に比べて非常に小さいので，熱平衡状態の密度行列は $Z$ 基底において非常に対角に近く，純粋状態 $|00\ldots0\rangle$, $|00\ldots01\rangle$, ..., $|11\ldots1\rangle$ の混合であると解釈できる．与えられた密度行列に対して解き方が無限にあるので，各アンサンブル要素の真の物理状態が実際に何であるかが議論すべき問題である．原理的にアンサンブルの要素（つまり各分子）にアクセスできれば，NMR で真の物理状態が測定できるが，実験的に難しい．

**演習 7.36:（熱平衡 NMR 状態）** $n=1$ に対して熱平衡状態は次式であることを示せ．

$$\rho \approx 1-\frac{\hbar\omega}{2k_{\mathrm{B}}T}\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}, \tag{7.141}$$

また $n=2$（および $\omega_A \approx 4\omega_B$）に対して次式が成立することを示せ．

$$\rho \approx 1-\frac{\hbar\omega}{4k_{\mathrm{B}}T}\begin{bmatrix}5 & 0 & 0 & 0\\ 0 & 3 & 0 & 0\\ 0 & 0 & -3 & 0\\ 0 & 0 & 0 & -5\end{bmatrix}. \tag{7.142}$$

**磁化の読み出し**

実験の主要な出力は自由誘導減衰信号であり，数式的に次式で与えられる：

$$V(t) = V_0 \ \mathrm{tr}\left[e^{-iHt}\rho e^{iHt}(iX_k+Y_k)\right], \tag{7.143}$$

ここで $X_k$ と $Y_k$ は $k$ 番目のスピンにのみ作用し，$V_0$ はコイルの形状，共振器の Q，試料体積で決まり，最大磁束に依存する定数因子である．この信号は $\hat{x}$ - $\hat{y}$ 平面内の試料の磁化を検出するピックアップコイルから生じる．実験室フレームで信号は核スピンの歳差周波数 $\omega_0$ で振動する．通常 $V(t)$ は $\omega_0$ にロックした発振器と混合して差周波を取り出し，最終信号を Fourier 変換して図 7.17 に示すように表示する．

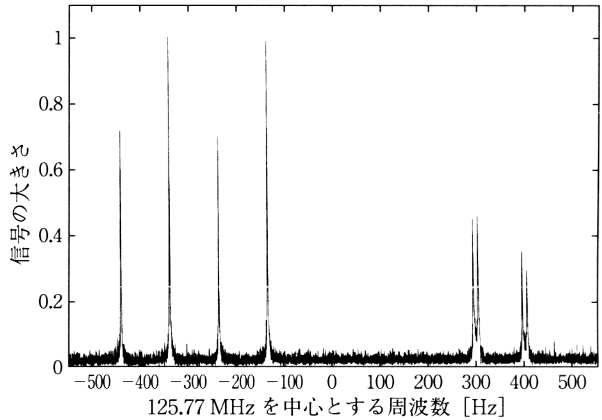



**図 7.17:** $^{13}$C のラベルを付した 3 塩化エチレンの炭素スペクトル．左側の 4 本のスペクトルは陽子に直接結合した炭素原子核から生じる．4 本となるのは陽子との結合と第 2 の炭素原子核との結合によるものであり，後者自身の信号は右側の狭い間隔の 4 本の線で表される．第 2 の炭素原子は最初の炭素よりさらに陽子から離れており，したがって両者の結合は弱い．

**演習 7.37:**（結合スピンの **NMR** スペクトル） $H = JZ_1Z_2$ と

$$\rho = e^{i\pi Y_1/4}\,\frac{1}{4}\,\left[1 - \beta\hbar\omega_0(Z_1 + Z_2)\right] e^{-i\pi Y_1/4}$$

に対する $V(t)$ を求めよ．もし Hamiltonian が $H = JZ_1(Z_2 + Z_3 + Z_4)$（であり初期密度行列が上と同様）ならば，最初のスピンのスペクトルは何本の線から成るか？ またそれらの相対的大きさはどうか？

### コヒーレンス劣化

NMR に対するこれまでの簡単なモデルでは触れなかったが，自由誘導減衰の主な性質は，磁化信号が指数関数的に減衰することである．この理由の 1 つは静磁界の不均一性にあり，これがあると試料の一部の歳差スピンが他の部分と位相ずれを起こす．不均一性の効果は原理上可逆であるが，他に本質的に非可逆な位相乱れを起こす原因，例えばスピン・スピン結合に起因する効果もある．もう 1 つの非可逆機構はスピンが環境温度と熱平衡になる機構であり，エネルギー移行を伴う．単一 q ビットに対してこれらの効果は現象論的に密度行列変換モデルで表現できる：

$$\begin{bmatrix} a & b \\ b^* & 1-a \end{bmatrix} \to \begin{bmatrix} (a-a_0)e^{-t/T_1}+a_0 & be^{-t/T_2} \\ b^*e^{-t/T_2} & (a_0-a)e^{-t/T_1}+1-a_0 \end{bmatrix}, \tag{7.144}$$

ここで $T_1$ と $T_2$ をそれぞれスピン・格子緩和時間 (spin-lattice relaxation time)（または「縦緩和時間」），スピン・スピン緩和時間 (spin-spin relaxation time)（または「横緩和時間」）と呼ぶ．$a_0$ は熱平衡状態を表す．これらは古典的非平衡状態と量子重ね合せの寿命に関する重要な時間スケールを規定する．NMR システムにおける $T_1$ と $T_2$ を計算する理論ツールはよく研究されており，NMR を使って異なる化学種の区別をするうえでこれらの測定は重要な働きをする．

$T_1$ と $T_2$ を測定する実験手法はNMR においてよく知られている．$R_x = e^{-i\pi X/4}$ は $\hat{x}$ の回りの 90° パルスであるとする．$T_1$ を測定するには $R_x^2$ を適用し，時間 $\tau$ だけ待ち，次に $R_x$ を適用する．最初のパルスでスピンが 180° 反転し，その後平衡状態に向かって時間 $\tau$ だけ緩和し（これを可視化すると基底状態である Bloch 球の頂点に向けて減衰する Bloch ベクトルで表せる），最後の 90° パルスで磁化が $\hat{x}$-$\hat{y}$ 平面に回転しそこで検出される．この**反転・回復**実験で測定された磁化 $M$ は指数関数 $M = M_0\big[1-2\exp(-\tau/T_1)\big]$ で $\tau$ と共に減衰することがわかっている．$T_2$ を測定するには 1 次近似でピークの線幅を測定すればよい．Carr-Purcell-Meiboom-Gill の方法と呼ぶもっと良い方法がある．この方法では $R_x$ 回転を加え，次に「時間 $\tau/2$ だけ待ち，$R_x^2$ を加え，時間 $\tau/2$ だけ待ち，$R_x^2$ を加え，$\cdots$」というプロセスを $k$ 回繰り返す．この 180° パルス列により結合を「再収束」(refocus) させ（7.7.3 項），$B_0$ 磁界の不均一を部分的に相殺してシステムの $T_2$ をより良く推定することができる．観測される磁化は $M = M_0 e^{-k\tau/T_2}$ で減衰する．

### 多スピン Hamiltonian

NMR Hamiltonian の議論をまとめると，$n$ 個の結合スピンシステムに対する $H$ は次のように書ける：

$$H = \sum_k \omega_k Z_k + \sum_{j,k} H_{j,k}^J + H^{\mathrm{RF}} + \sum_{j,k} H_{j,k}^{\mathrm{D}} + H^{\mathrm{env}}, \tag{7.145}$$

ここで第 1 項は磁界中のスピンの自由歳差運動，$H^{\mathrm{D}}$ は式 (7.136) の磁気双極子結合，$H^{J}$ は式 (7.137) の「$J$ 結合」，$H^{\mathrm{RF}}$ は式 (7.135) の外部印加 RF 磁界の効果，$H^{\mathrm{env}}$ は式 (7.144) のようなコヒーレンス劣化を引き起こす環境との相互作用を記述する．

このHamiltonian の操作法に関する基本原理を理解するために，次に続く議論では簡単化した Hamiltonian：

$$H = \sum_k \omega_k Z_k + \sum_{j,k} Z_j \otimes Z_k + \sum_k [g_k^x(t) X_k + g_k^y(t) Y_k] \qquad (7.146)$$

を考えれば十分であることがわかる．一般の式 (7.145) も同じ考えで取り扱うことができる．

## 7.7.3 量子計算

量子情報処理では適切な初期状態に準備したシステムに対してユニタリー変換を行う必要がある．現在のシステムに関して 3 つの疑問が生じる：第 1 は式 (7.146) で記述される $n$ 個の結合スピンシステムに対して任意のユニタリー変換をどのように実行するのか？ 第 2 に (7.140) で記述された NMR システムの熱平衡状態をどのように計算の適切な初期状態として使うのであろうか？ 3 番目に前の 3 つの章で調べた量子アルゴリズムでは出力結果を得るのに射影測定を要求していたが，NMR で容易にできるのはアンサンブル平均だけである．このアンサンブル読み出し問題をどう取り扱えるのか？ 本項でこれらの疑問に答える．

### 再収束

式 (7.146) の Hamiltonian を用いて任意のユニタリー変換を行う際に利用できる最も興味深いテクニックは，おそらく NMR 技術で知られている**再収束**(refocusing) であろう．2 個のスピンに対する Hamiltonian $H = H^{\mathrm{sys}} + H^{\mathrm{RF}}$ を考える．ここで

$$H^{\mathrm{sys}} = aZ_1 + bZ_2 + cZ_1 Z_2. \qquad (7.147)$$

7.7.2 項で示したように適切な周波数の大きな RF 磁界を加えたとき，次式が十分良い近似となる：

$$e^{-iHt/\hbar} \approx e^{-iH^{\mathrm{RF}}t/\hbar}. \tag{7.148}$$

これにより優れた忠実度で任意の単一 q ビット演算が実行できる．スピン 1 に対して

$$R_{x1} = e^{-i\pi X_1/4} \tag{7.149}$$

を $\hat{x}$ 軸の回りの 90° 回転と定義し，スピン 2 に対しても同様の定義をする．180° 回転 $R_{x1}^2$ は次のような特別の性質を持つことが容易に証明できる：

$$R_{x1}^2 e^{-iaZ_1 t} R_{x1}^2 = e^{iaZ_1 t}. \tag{7.150}$$

Bloch 球上のある点を同時に出発した異なる周波数のスピンが，Bloch 球上の同じ点に同時に戻って来るように時間発展を逆転させるので，この方法を再収束と呼び，この方法で加える 180° パルスを再収束パルスと呼ぶ．上式で $a$ は（スピン 1 に働くオペレータを含まない限り）定数であると同時にオペレータにもなり得る．したがって

$$e^{-iH^{\mathrm{sys}}t/\hbar} R_{x1}^2 e^{-iH^{\mathrm{sys}}t/\hbar} R_{x1}^2 = e^{-2ibZ_2 t/\hbar}. \tag{7.151}$$

スピン 2 に対して別の再収束パルスの組を加えるとこの残留項も取り去ることができる．したがって，再収束はスピン間の結合した時間発展を取り除き，すべての時間発展を完全に取り除く便利なテクニックである．

**演習 7.38:（再収束）** 式 (7.150) が成り立つことを陽に示せ．（Pauli の行列の反交換関係を用いよ．）

**演習 7.39:（3 次元の再収束）** **任意の**単一スピン Hamiltonian $H^{\mathrm{sys}} = \sum_k c_k \sigma_k$ のもとで起きる時間発展を再収束するにはどのようなパルスの組を用いればよいか？

**演習 7.40:（双極子相互作用の再収束）** 2 個のスピンの双極子結合 $H_{1,2}^{\mathrm{D}}$ を式 (7.138) の簡単な形に変えるのに用い得る一連のパルス列を与えよ．

### 制御 NOT ゲート

再収束パルスと単一 q ビットパルスを用いると制御 NOT ゲートを簡単に実現できる．式 (7.147) の Hamiltonian を有する 2 個のスピンシステムに対して，これを行う方法を示そう．式 (7.46) の構成から次のユニタリー変換を実現できれば十分であるのがわかる：

$$U_{CZ} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}. \tag{7.152}$$

$\sqrt{i}e^{iZ_1Z_2\pi/4}e^{-iZ_1\pi/4}e^{-iZ_2\pi/4} = U_{CZ}$ なので，時間 $\hbar\pi/4c$ の 1 回の時間発展と数回の単一 q ビットパルスによって制御 NOT が直ぐに得られる．

**演習 7.41:（NMR 制御 NOT）** Hamiltonian (7.147) のもとで時間発展する 2 個のスピン間で，制御 NOT を実現する一連の q ビット回転の列を明示的に与えよ．式 (7.46) から始めてもよいが，その結果を簡単にできて，単一 q ビット回転の数を減らすことができる．

### 時間，空間および論理ラベル

スピンシステムに対して RF パルスを用いて，良い忠実度で任意のユニタリー変換が実現できることは，NMR を量子計算に用いるときの最大の魅力の 1 つである．しかし大きな欠点は，通常初期状態が式 (7.140) の熱平衡状態であるという事実である．この状態が高エントロピーであるにもかかわらず，ある犠牲を払えば量子計算を行うことができる．これを行う 2 つの方法が時間ラベルと論理ラベルである．

時間ラベル (temporal labeling) あるいは時間平均 (temporal averaging) とも呼ぶ方法は，2 つの重要な事実に基づいている：量子演算は線形であり NMR で測定される観測量はトレースが 0 になる（量子測定の背景については 2.2.5 項（第 I 巻）参照）．2 個のスピンシステムが次の密度行列から出発すると考える：

$$\rho_1 = \begin{bmatrix} a & 0 & 0 & 0 \\ 0 & b & 0 & 0 \\ 0 & 0 & c & 0 \\ 0 & 0 & 0 & d \end{bmatrix}, \tag{7.153}$$

ここで $a$, $b$, $c$, $d$ は $a+b+c+d=1$ を満たす任意の正の数である．制御 NOT ゲートで構成した置換回路 $P$ を用いて分布を入れ替えた状態：

$$\rho_2 = P\rho_1 P^\dagger = \begin{bmatrix} a & 0 & 0 & 0 \\ 0 & c & 0 & 0 \\ 0 & 0 & d & 0 \\ 0 & 0 & 0 & b \end{bmatrix} \tag{7.154}$$

と，同様にして作った状態：

$$\rho_3 = P^\dagger \rho_1 P = \begin{bmatrix} a & 0 & 0 & 0 \\ 0 & d & 0 & 0 \\ 0 & 0 & b & 0 \\ 0 & 0 & 0 & c \end{bmatrix} \tag{7.155}$$

が得られる．これらの各状態にユニタリーな量子計算 $U$ を適用すると（異なる時刻に別々に実験を行って）$C_k = U\rho_k U^\dagger$ が得られる．線形性を用いると

$$\sum_{k=1,2,3} C_k = \sum_k U\rho_k U^\dagger \tag{7.156}$$

$$= U\Big[\sum_k \rho_k\Big]U^\dagger \tag{7.157}$$

$$= (4a-1)U \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} U^\dagger + (1-a) \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}. \tag{7.158}$$

NMR では $\mathrm{tr}(M) = 0$ となる観測量 $M$（例えば Pauli の $X$ や $Y$）だけが測定されるので

$$\mathrm{tr}\Bigl(\sum_k C_k M\Bigr) = \sum_k \mathrm{tr}\,(C_k M) \tag{7.159}$$

$$= (4a-1)\ \mathrm{tr}\left( U \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} U^\dagger M \right) \tag{7.160}$$

$$= (4a-1)\ \mathrm{tr}(U|00\rangle\langle 00|U^\dagger). \tag{7.161}$$

これら 3 つの実験で測定された信号の和は，もしも元のシステムが任意の状態 (7.153) ではなく，純粋状態 $|00\rangle\langle 00|$ に準備されていた場合に得られるであろう結果に比例した結果を与える．コヒーレンス劣化を起こすことなく，ユニタリー変換を行うのに十分な長いコヒーレンス時間が確保できれば，和をとる実験回数を十分多く行うことができて，如何なるサイズのシステムが任意の状態に準備されてもこれが常に実行可能である．異なる $C_k$ の実験を 3 つの異なるシステムを用いて同時に行うことや，1 つのシステムの異なる部分を用いて行うことも可能であることを注意しておく．1 つの試料内で系統的に変化する傾きを持った磁界を加えて実験を行うことも可能であり，この変形したテクニックを空間ラベル (spatial labeling； 空間平均，spatial averaging) と呼ぶ．

**演習 7.42:（時間ラベルのための置換）** 式 (7.153) の $\rho_1$ を式 (7.154) の $\rho_2$ に変換するに必要な置換 $P$ と $P^\dagger$ を実行する量子回路を与えよ．

論理ラベル (logical labeling) は同様の観測に基づくものであるが，多数回の実験を必要としない．3 つのほぼ同様なスピンから成るシステムが次の状態にあるとする：

$$\rho = \delta I + \alpha \begin{bmatrix} 6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -6 \end{bmatrix} \tag{7.162}$$

$$\approx \left( \delta' I + \alpha' \begin{bmatrix} 2 & 0 \\ 0 & -2 \end{bmatrix} \right)^{\otimes 3}, \tag{7.163}$$

ここで $\delta I$ は（トレースが 0 の観測量なので）観測されない背景分布，$\alpha \ll \delta$ は小さい定数を表す．次に置換を実行するユニタリー演算 $\tilde{P}$ を適用すると

$$\rho' = \tilde{P}\rho\tilde{P}^\dagger = \delta I + \alpha \begin{bmatrix} 6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -6 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 \end{bmatrix}. \tag{7.164}$$

この行列の上の $4 \times 4$ のブロックは次の形となる：

$$\begin{bmatrix} 6 & 0 & 0 & 0 \\ 0 & -2 & 0 & 0 \\ 0 & 0 & -2 & 0 \\ 0 & 0 & 0 & -2 \end{bmatrix} = 8|00\rangle\langle 00| - 2I, \tag{7.165}$$

ここで $I$ は $4 \times 4$ の単位行列である．時間ラベルの場合と同様にこのような状態（いまの場合は $|000\rangle$, $|001\rangle$, $|010\rangle$, $|011\rangle$ の多重状態）に対して計算を行うと，あたかも元の状態が純粋状態 $|00\rangle\langle 00|$ に初期化されていたときに得られるであろう

結果に比例した結果を出力する！ 実験的に $\tilde{P}$ を実行してこの多重状態から信号を分離することも可能である．

$\rho = 2^{-n}(1-\epsilon)I + \epsilon U|00\ldots0\rangle\langle 00\ldots0|U^\dagger$（$U$ は任意のユニタリーオペレータ）の形をした状態は「実効的純粋状態」(effective pure state) もしくは「疑似純粋状態」(pseudopure state) という．$n$ は q ビットの数であるが，Hilbert 空間の次元は一般に 2 のベキである必要はない．このような状態を作るための方法は沢山あるが，すべてなにがしかのコストを必要とする．この点について 7.7.4 項でもう一度扱う．実効的純粋状態によってゼロ温度の振る舞いを観測することができる．これが NMR 量子計算で用いられている方法である．

**演習 7.43:（論理ラベルに対する置換）** 式 (7.163) の $\rho$ を式 (7.165) の $\rho'$ に変換するに必要な置換 $\tilde{P}$ を実行する量子回路を与えよ．

**演習 7.44:（$n$ 個のスピンに対する論理ラベル）** $n$ 個のほとんど同じスピンが Zeeman 周波数 $\hbar\omega$ を有し，状態 $\rho$ と温度 $T$ で熱平衡にあるとする．論理ラベルを使って $\rho$ から構成できる最大の実効的純粋状態は何か？（ヒント：$n/2$ の Hamming 重みを持つラベルの状態の利点を使え．）

### 量子アルゴリズムの結果のアンサンブル読み出し

式 (7.146) の Hamiltonian を有する $n$ 個のスピンシステムに対して，任意のユニタリー変換を実行する方法について調べ，低エントロピーの基底状態として振る舞う明確に定義された入力を，熱平衡状態から作る方法がわかった．しかし量子計算の要請を完全に満たすには，システムを測定して計算結果を読み出す方法がなければならない．困難なのは典型的量子アルゴリズムの出力がランダムな数であり，その分布が問題を解く情報を与える．残念ながらランダム変数の平均値は必ずしも妥当な情報をもたらさない．もしも量子アルゴリズムが何の変更もなく NMR 量子コンピュータに適用されたならば，$n$ 個のスピンを有する単一分子でなく分子の大きなアンサンブルに適用するので，この平均値が出力となってしまう．

この困難さは次の例でよくわかる．量子素因数分解アルゴリズムは出力としてランダムな有理数 $c/r$ を作り出す．ここで $c$ は未知の整数，$r$ は望む結果（整数）

である．通常は射影測定を用いて $c/r$ を得て，次に古典的な連分数展開を実行して高い確率で $r$ を得る（5.3.1項）．この結果を元の問題に戻して答をチェックし，もし駄目ならば全体のアルゴリズムをもう一度繰り返す．しかし不幸にしてアンサンブル平均しか得られなければ，$c$ はほとんど一様に分布しているので平均値 $\langle c/r \rangle$ は意味のない情報しか与えない．

この問題に対する簡単な解決法は，量子計算の後に必要な古典的な後処理ステップを設けることであり，この方法は隠れ部分群問題（5章）に基づく全量子アルゴリズムに適用できる．これが常に可能であるのは量子計算が古典計算を包含するからである．上の例では単に各量子コンピュータ（各分子）に連分数展開を行うよう要求すればよい．結果は各量子コンピュータで検証され，検証に成功したコンピュータだけが出力を出す．最後にアンサンブル平均を測定すれば $\langle r \rangle$ が得られる．

### 7.7.4　実　験

NMRによるアプローチで感激するのは，量子計算と量子情報タスクの小さな事例を直ぐに実験で実現できることである．NMRに関して最後となるこの項ではこれまでに行われた状態トモグラフィーの実証，基本的論理ゲート要素，量子探索アルゴリズムの3つの実験について簡潔に述べる．この方法の欠点についてもまとめる．

#### 状態トモグラフィー

量子コンピュータのデバグ (debug) はどうするのであろうか？ 古典コンピュータならば異なる時間における内部状態を測定して解析できる．同様に量子コンピュータでも本質的なテクニックは密度行列を測定できる能力であり，これを**状態トモグラフィー**(state tomoraphy) と呼ぶ．

単一qビットの密度行列を次のように表す：

$$\rho = \frac{1}{2}\Big[1 + \sum_k r_k \sigma_k\Big], \tag{7.166}$$

ここで $\sigma_k$ は Pauli の行列，$r_k$ は3次元の実数ベクトルである．Pauli の行列の

トレース直交性より

$$\mathrm{tr}(\sigma_k \sigma_j) = 2\delta_{kj}, \tag{7.167}$$

$\rho$ は 3 つの測定結果から再構成される：

$$r_k = \langle \sigma_k \rangle = \mathrm{tr}(\rho \sigma_k). \tag{7.168}$$

適切な単一 q ビットパルスを加えた後で，NMR の通常の観測量 (7.143) を測定すると，$\langle \sigma_k \rangle$ を決定することができ，したがって $\rho$ が得られる．同様の結果はスピンの数が多いときにも成立する．実際には単位行列からの $\rho$ の偏差（トレースが 0 となる）を測定するのが便利であり，これを偏差密度行列 (deviation density matrix) と呼ぶ．2 つと 3 つのスピンを有するシステムに対する実験例を図 7.18 に示す．

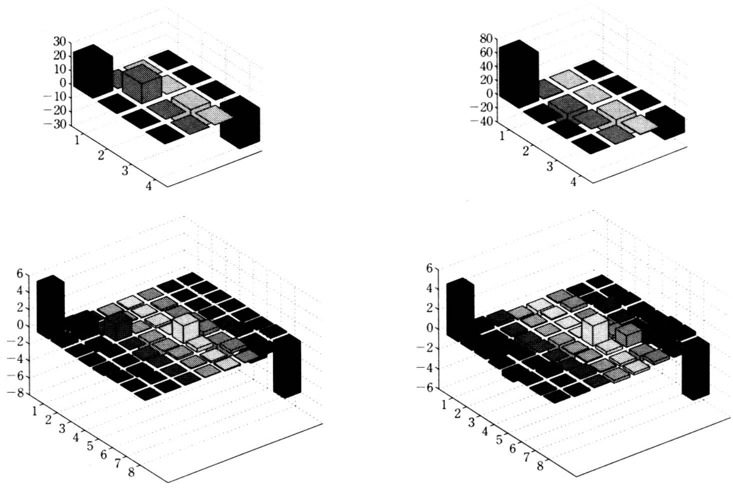


**図 7.18:** 実験で求めた偏差密度行列．縦スケールは任意で実数部のみを示す．虚数部はすべて比較的小さい．左上： 11.78 テスラの磁界中のクロロフォルム分子（$^{13}$CHCl$_3$）の陽子と炭素原子核の 2 - q ビット熱平衡状態．0.5 ミリリットル，200 ミリモルの試料を脱気アセトン-$d_6$ で希釈して薄壁 5 mm のガラス管に火炎封止．右上： クロロフォルムにおいて式 (7.161) のように時間ラベルで 2 - q ビットの実効的純粋状態を作成．左下： トリフルオロエチレンの 3 つの原子核の 3 - q ビット熱平衡状態．右下： 式 (7.164) の論理ラベルを使って 3 つのスピンシステムから作った実効的純粋状態．

**演習 7.45:**（**NMR による状態トモグラフィー**）　電圧測定

$$V_k(t) = V_0 \ \mathrm{tr}\left[e^{-iHt} M_k \rho M_k^\dagger e^{iHt} (iX_k + Y_k)\right]$$

が実験 $k$ の結果であるとする．2 つのスピンに対して，$M_0 = I$，$M_1 = R_{x1}$，$M_2 = R_{y1}$，$M_3 = R_{x2}$，$M_4 = R_{x2}R_{x1}$，$M_5 = R_{x2}R_{y1}$ 等の 9 回の実験によって，$\rho$ を再構成するに十分なデータが得られることを示せ．

**演習 7.46:** 3 つのスピンに対して何回の実験で十分か？ それは必要か？

### 量子論理ゲート

クロロフォルムの陽子・炭素の 2 - q ビットシステムは多くの理由で，単一 q ビットゲートおよび 2 - q ビットゲートを実証するのに優れたシステムである．約 11.8 テスラの磁界中で，2 つのスピン周波数が約 500 MHz と約 125 MHz と十分離れているので容易に扱える．2 つの原子核の $J$ 結合周波数 215 Hz も便利である．これは単一 q ビット RF パルスに必要な時間スケールよりはるかに遅いが，緩和時間スケールより十分速い．典型的実験では陽子と炭素の $T_1$ はそれぞれ約 18 秒と 15 秒であり，$T_2$ は 7 秒と 0.3 秒である．炭素の $T_2$ が短いのは 3 個の 4 重極塩素原子との相互作用のせいであるが，最短の $T_2$ 寿命と $J$ 結合の積をとると，量子コヒーレンスが失われるまでにおよそ 60 ゲートが実行できることがわかる．

2 つのスピンシステムの Hamiltonian は，式 (7.147) の表現で非常によく近似できるが，実験的工夫により大幅に簡単化できる．2 つの発振器を陽子と炭素の回転周波数に正確に同調すると，発振器で規定される回転フレームにおいて簡単化された Hamiltonian は：

$$H = 2\pi\hbar J Z_1 Z_2, \tag{7.169}$$

ここで $J = 215$ Hz である．この Hamiltonian によって制御 NOT ゲートが非常に簡単に実現できる．単一 q ビットの位相を除いて等価な制御 NOT 演算を行う回路を，Bell 状態を生成する回路と実験の測定出力と合わせて図 7.19 に示す．

**演習 7.47:**（**NMR 制御 NOT ゲート**）　図 7.19 の左上に示す回路は単一 q ビットの位相を除いて制御 NOT ゲートを実行することを証明せよ．つまりこ

れは古典的入力状態に正確に作用し，さらに単一 q ビット $R_z$ 回転を付加して適用すれば，正確な制御 NOT ゲートにできる．同じ構成ブロックを用いて，正確な制御 NOT ゲートを実現する別の回路を与えよ．

**演習 7.48:** 図 7.19 の左下に示す回路は，Bell 状態 $(|00\rangle - |11\rangle)/\sqrt{2}$ を作り出すことを証明せよ．

**演習 7.49:（NMR 交換ゲート）** NMR の化学への重要な応用はスピンによる結合の測定，つまり分子中で陽子，炭素，燐原子のどれが最近接かを測定することである．これを行う 1 つのパルス列を INADEQUATE（incredible natural abundance double quantum transfer experiment の略 — NMR には素晴らしく独創的な略語が多い．）と呼ぶ．量子計算の言葉では任意の 2 つの共鳴間で単に制御 NOT の適用を試みることと理解できる．もし制御 NOT が働けば，2 つの原子核は隣接している．その他に，TOCSY（total correlation spectroscopy の略）のパルス列で用いられる構成要素は交換演

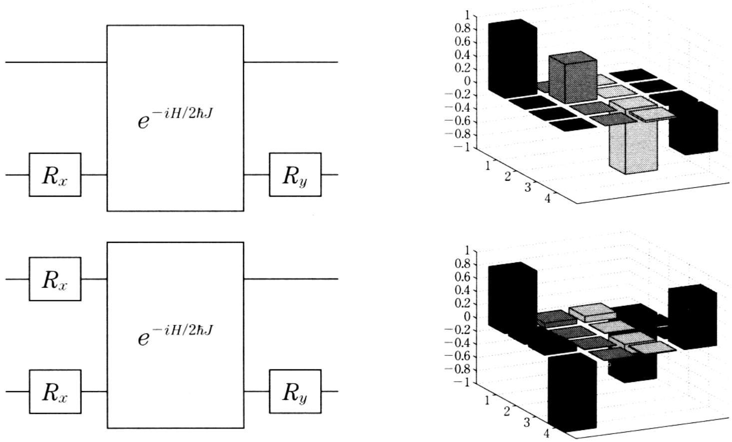



**図 7.19:** NMR で実現した量子回路（左）と，実験で測定した出力の偏差密度行列の実数部（右）．これらの回路で $R_x$ と $R_y$ は約 10 マイクロ秒の RF パルスで実行される $\hat{x}$ と $\hat{y}$ の回りの 90° 回転を実行する単一 q ビットゲートを表し，$e^{-iH/2\hbar J}$ で表した 2 つの q ビットの箱は時間 $1/2J \approx 2.3$ ミリ秒の自由な時間発展を表す．上：制御 NOT 回路と熱平衡状態入力に対する出力．制御 NOT ゲートに対する古典的真理値表から期待されるように，$|10\rangle$ と $|11\rangle$ の対角要素の交換を示す．下：Bell 状態 $(|00\rangle - |11\rangle)/\sqrt{2}$ を作り出す回路と，実効的純粋状態 $|00\rangle$ が入力したときのその出力．

算であるが，量子ゲートで簡単に記述できるような完全なものではない！$e^{-iH/2\hbar J}$，$R_x$，$R_y$ 演算のみを使って交換ゲートを実現する量子回路を構成せよ．(図 1.7（第 I 巻）の回路から出発するとよい.)

## 量子アルゴリズム

もう 1 つの NMR 量子計算の簡単な例は Grover の量子探索アルゴリズムである．4 要素（$n = 2$ - q ビット）のサイズの問題に対して，集合 $x = \{0,\ 1,\ 2,\ 3\}$ が与えられ，$f(x_0) = 1$ なる 1 つの値 $x_0$ を除いて $f(x) = 0$ とする．ゴールは $x_0$ を見出すことであり，古典的にこれを行えば $f(x)$ を平均 2.25 回評価すれば達成できる．これに比べて量子アルゴリズムでは $f(x)$ を 1 回評価すると $x_0$ が見つかる（6 章，特にコラム 6.1 参照)．

3 つのオペレータが必要となる：（関数 $f(x)$ に基づき位相反転をする）オラクルオペレータ $O$，2 個の q ビットに働く Hadamard オペレータ $H^{\otimes 2}$，および条件付き位相シフトオペレータ $P$ である．オラクル $O$ は $x_0$ に対応する基底要素の符号を反転する．$x_0 = 3$ とするとこれは

$$O = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}. \tag{7.170}$$

$t = 1/2J$（クロロフォルムでは 2.3 ミリ秒）の間隔の時間発展 $e^{-iH/2\hbar J}$ の周期を $\tau$ と表すと，$x_0 = 3$ の場合に（無関係な全体の位相因子を除いて）$O = R_{y1}\bar{R}_{x1}\bar{R}_{y1}R_{y2}\bar{R}_{x2}\bar{R}_{y2}\ \tau$ であることがわかる．$H^{\otimes 2}$ は 2 つの単一 q ビット Hadamard 演算 $H_1 \otimes H_2$，ここで $H_k = R_{xk}^2\bar{R}_{yk}$ である．オペレータ $P$：

$$P = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} \tag{7.171}$$

は $P = R_{y1}R_{x1}\bar{R}_{y1}R_{y2}R_{x2}\bar{R}_{y2}\ \tau$ として簡単に実現できる．これを用いて Grover

の反復 $G = H^{\otimes 2}PH^{\otimes 2}O$ を構築する．明らかに相殺する不必要な演算を消去すると，このオペレータは直ちに簡単化できる（演習 7.51 参照）．初期状態に Grover の反復を $k$ 回適用した後の状態を $|\psi_k\rangle = G^k|00\rangle$ とする．振幅は $\langle x_0|\psi_k\rangle \approx \sin((2k+1)\theta)$ であることがわかる．ここで $\theta = \arcsin(1/\sqrt{2})$ である．この周期性が量子探索アルゴリズムの基本的性質であり，実験で検証すべき点である．2 個の q ビットで $x_0 = 3$ の場合，$|11\rangle = |\psi_1\rangle = -|\psi_4\rangle = |\psi_7\rangle = -|\psi_{10}\rangle$，つまり全体の符号を無視すれば周期 3 が期待される．

**演習 7.50:** 単一 q ビット回転と $e^{-iH/2\hbar J}$ だけを用いて，$x = 0,\ 1,\ 2$ に対するオラクル $O$ を実行する量子回路を見出せ．

**演習 7.51:** 隣り合う単一 q ビット回転を適切に相殺することにより Grover の反復を簡単化し，$x_0$ の 4 つの可能な場合に対して次式が得られることを示せ．

$$G = \begin{cases} \bar{R}_{x1}\bar{R}_{y1}\bar{R}_{x2}\bar{R}_{y2}\ \tau\ R_{x1}\bar{R}_{y1}R_{x2}\bar{R}_{y2}\ \tau & (x_0 = 3) \\ \bar{R}_{x1}\bar{R}_{y1}\bar{R}_{x2}\bar{R}_{y2}\ \tau\ R_{x1}\bar{R}_{y1}\bar{R}_{x2}\bar{R}_{y2}\ \tau & (x_0 = 2) \\ \bar{R}_{x1}\bar{R}_{y1}\bar{R}_{x2}\bar{R}_{y2}\ \tau\ \bar{R}_{x1}\bar{R}_{y1}R_{x2}\bar{R}_{y2}\ \tau & (x_0 = 1) \\ \bar{R}_{x1}\bar{R}_{y1}\bar{R}_{x2}\bar{R}_{y2}\ \tau\ \bar{R}_{x1}\bar{R}_{y1}\bar{R}_{x2}\bar{R}_{y2}\ \tau & (x_0 = 0) \end{cases} . \quad (7.172)$$

図 7.20 に偏差密度行列 $\rho_{\Delta n} = |\psi_n\rangle\langle\psi_n| - \mathrm{tr}(|\psi_n\rangle\langle\psi_n|)/4$ の理論と実験結果を，$U$ を最初に 7 回繰り返したときに対して示す．期待通り $\rho_{\Delta 1}$ は $x_0 = 3$ に対応して明確に $|00\rangle$ 状態を示している．$x_0$ の他の値に対して繰り返した実験で同様の結果が得られている．各密度行列を測定するのにはトモグラフィーの再構成に 9 回，純粋状態の作成に 3 回，合計 $9 \times 3 = 27$ 回の繰り返しが必要である．

$n = 7$ の最長の計算に 35 ミリ秒の時間を要し，コヒーレンス時間内に十分納まっている．図 7.20 において Grover のアルゴリズムの周期性が明瞭に見られ，理論と実験が良い一致を示している．1 回の測定に対して良好な信号対雑音比（典型的には $10^4$ 対 1 以上）が得られた．数値シミュレーションによれば $7 \sim 44\%$ の誤差要因は，（重要さの順に）磁界の不均一，測定中の磁化の減衰，回転の較正誤差によるものである．

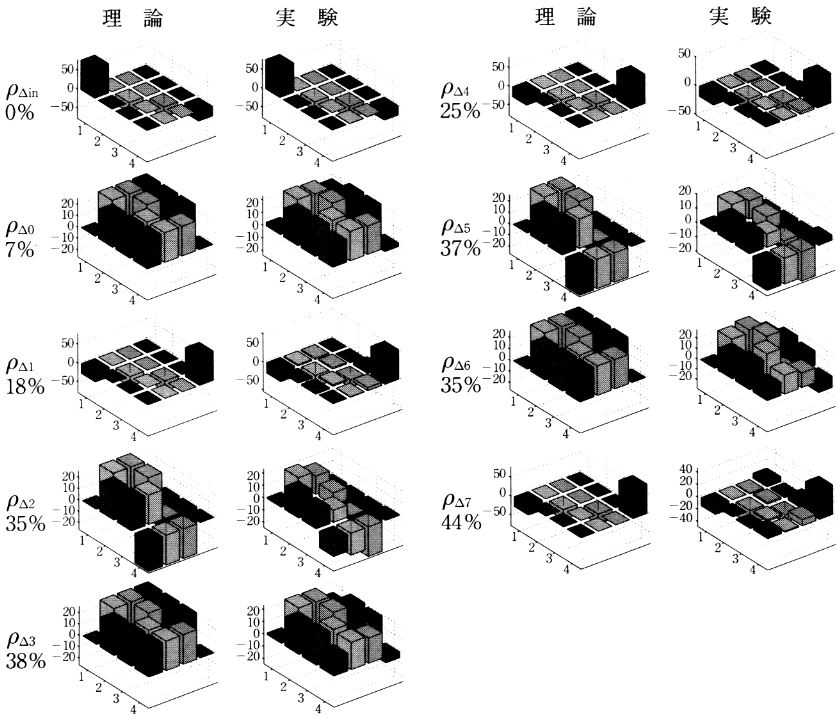



**図 7.20:** クロロフォルムの水素と炭素に対して行われた 7 ステップ Grover アルゴリズムの，理論および実験のよる偏差密度行列（単位は任意）．3 の繰り返し周期を持つ 2 周期が明瞭に見られる．実数部のみをプロットしている（虚数部は理論ではゼロ，実験では 12% 以下の寄与である）．相対誤差 $\|\rho_{\text{theory}} - \rho_{\text{expt}}\|/\|\rho_{\text{theory}}\|$ を % 数値で示している．

## 欠　点

量子計算をバルクアンサンブルの NMR で実行する試みでは，7 - q ビットまでのシステムで量子アルゴリズムと量子情報のタスクを実証しており，これは真に印象的である．しかしこの方法の核心である時間，空間，論理ラベルのテクニックには重大な制約がある．

これらラベル化技術の本質的な目的は，熱平衡状態の $|00\ldots0\rangle$ 成分（あるいは他の標準的な高存在確率の状態）にたまたま存在するスピンの部分集合からの信号を分離することにある．これを行うのに時間および空間ラベルでは信号を加え合わせて，望む状態以外をすべて相殺する．論理ラベルでは Hibert 空間を犠

牲にして純粋状態を確保する．しかし用いる方法に関係なく熱平衡状態における $|00\ldots0\rangle$ 成分の確率：

$$p_{00\ldots0} = \frac{1}{\mathcal{Z}}\langle 00\ldots0|e^{-\beta H}|00\ldots0\rangle \tag{7.173}$$

は増加することはない．$H = \sum_k \omega Z_k$ とおくと，$n$ 個のスピンを持つ分子で $p_{00\ldots0}$ は $n2^{-n}$ に比例する．これが意味するところは初期温度を一定とすると，ラベル化技術で q ビット数が実効的純粋状態に「蒸留」されるに伴って，全信号が**指数関数的に減少**する．

もう 1 つの制約が量子コンピュータとして分子を用いることから生じる．分子構造はコンピュータ**アーキテクチャ**の役割を果たし，どの q ビット対（またはグループ）が互いに相互作用するかを決める（同様の類推では RF パルスがソフトウェアに相当する）．全 q ビットが必ずしもよく結合しているわけではない！ 再収束を行う以外に相互作用を切ることはできないので，これは 2 重の意味で重要である．さらに q ビットへのアクセスは周波数で区別して行うが，原子核の数が増えるとこれは急速に困難になる．この問題の解決は存在しており，セルオートマトン型のアーキテクチャを用いることである．例えば 1 次元の鎖 $X-A-B-C-A-B-C-\cdots-A-B-C-Y$ において，両端は識別できるが中は規則的な順序の繰り返しになっている．この構造は異なる文字しかアドレスできず非常に制約された計算モデルであるかに見える．しかし実際はこれが普遍的であることがわかっており，多項式的な低速化が生じるだけである．もちろん量子探索アルゴリズムのような平方根の高速化しかできないタスクを実行するには，低速化の正確な量が重要になる．

ラベル化技術の制約を回避する方法も存在する．1 つの可能性は何か物理的機構を使って原子核を分極させることである．これは（図 7.8 で示したイオン冷却法と同様な）光ポンピングを使って行われ，ルビジウム原子の電子状態を分極させ，次に短寿命の van der Waaks 分子を形成してその分極をクセノン原子核に伝達する．これはヘリウムに対しても行われた．技術的に困難であるが，同じことを分子に対して行うことが考えられる．別の可能性は異なるラベル化法を用いることである．論理ラベルは本質的には圧縮アルゴリズムであり，アンサンブル要素を捨て去ることによってアンサンブル中の 1 つの状態の相対確率を増加させる．この方法を改善して初期温度 $T$ で確率が $p = (1-e^{-\Delta E/k_{\mathrm{B}}T})/2$（$\Delta E$ はス

ピン反転エネルギー）にある $n$ 個のスピンを有する分子から，エントロピー限界の $nH(p)$ 個の純粋な q ビットを得る方法が開発されている．この方法は指数関数的な犠牲は払わないで基本的演算を多項式数用いるだけで圧縮を達成できる．しかしこれは $p$ が比較的小さくなければ効率が悪く，良いソレノイド磁石を使って今日得られる値は $p \approx 0.4999$ である．

これらの欠点にもかかわらず NMR は量子アルゴリズムのためのテストベッドを提供し，他の実現方法ならば量子計算を行うためにこれから実現しなければならない基本テクニックを，実例で示すことができる．量子計算と量子情報タスクの実証に用いられた分子を図 7.21 に示す．NMR の概念は化学，物理，技術，数学を結ぶ非常に豊かな分野であり，疑いなく分野間の革新が続くとこの技術は進展するであろう．

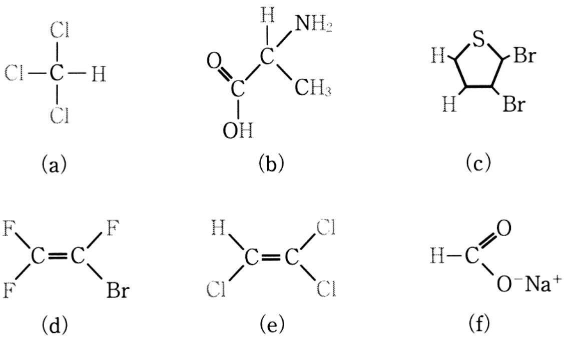



**図 7.21:** NMR でいろいろな量子計算と量子情報のタスクを実証するのに用いられた単純な分子．(a) クロロフォルム：陽子と炭素の 2 つの q ビットが Deutsch-Jozsa のアルゴリズムと 2 - q ビット量子探索の実行に用いられた．(b) アラニン：炭素骨格から成る 3 つの q ビットが誤り訂正の実証に用いられた．3 つの炭素は周囲の化学的環境が異なるので識別できることに注意（例えば，酸素原子の電気陰性度により隣接原子から電子が引き寄せられる）．(c) 2,3-ジブロモチオフェン：2 つの陽子から成る 2 つの q ビットが有限な深さの単純調和振動子の 4 準位シミュレーションに用いられた．ここでは 2 つの陽子が硫黄原子との距離が異なるために周波数で識別できる．(d) トリフルオロブロモメチレン：3 つのフッ素の 3 - q ビットが論理ラベルと重ね合せ状態 $(|000\rangle + |111\rangle)/\sqrt{2}$ 生成の実証に用いられた．(e) トリクロロエチレン：陽子と 2 つの炭素の 3 個の q ビットがテレポーテーションの実証に用いられ，陽子の状態が一番右の炭素の状態にテレポートされた．(f) 蟻酸ナトリウム：陽子と炭素の 2 個の q ビットが 2 - q ビットの量子誤り訂正符号の実証に用いられた．この分子でナトリウムラジカルは溶媒との交換の割合を温度で変化させて，2 つの q ビットの緩和時間 $T_2$ をほぼ等しく調整するために用いられている．

### NMR 量子コンピュータ

- **q ビット表現：** 原子核スピン．
- **ユニタリー時間発展：** 強い磁界中に置かれたスピンに磁界パルスを印加して，任意の変換を構成する．スピン間の結合は隣接原子間の化学結合により生じる．
- **初期状態の調製：** 強い磁界中にスピンを置いて分極させ，「実効的純粋状態」を作るテクニックを使用する．
- **読み出し：** 歳差運動をする磁気モーメントが誘起する電圧を測定する．
- **欠点：** 初期の分極が十分に高くなければ，実効的純粋状態の生成法により q ビット数に応じて信号が指数関数的に減少する．

## 7.8　他の実現法

本章では量子コンピュータを実現するために考え出された多くのアイディアのうちでほんの一部について述べてきた．ここで選んだものだけでも量子情報のロバストな表現，ユニタリー変換の適用，信頼できる入力状態，出力の測定等，すべての実現法に共通な基本的要請とその実現の困難さを示している．

単純調和振動子の例を用いて**ディジタル**表現の重要さを強調した．量子情報の各ユニットは（q ビット (qubit)，q トリット (qutrit)，q ディット (qudit) 等何であれ）**物理的に分離した**自由度を持っていなければならず，そうでなければ（エネルギーのような）リソースの利用が非効率になる．またこの例はこの章のそれ以降の部分を通じて，q ビット表現を学ぶ数学的基礎を与えてくれた．単一光子は理想に近い q ビットであるが，それらを相互作用させるに必要な非線形光学材料は，コヒーレンスの損失を起こすことなく実現するのが難しい．共振器 QED 技術は光子と相互作用する単一原子を用いてこの問題に対応することができる．もっと重要なことは，ここで 2 準位原子の概念と双極子選択則のように物理的対称性に基づく選択則を用いて q ビット表現を保護するアイディアを導入したことである．

このアイディアを拡張すると本来 2 準位しかないスピン 1/2 の粒子を使って q ビットを表現する考えに達する．これがトラップイオンを用いる方向であり，q ビットは電子と原子核のスピンに蓄積される．しかしこの方法の困難さはスピン

間の相互作用を仲介する質量中心の振動 — つまりフォノン— のコヒーレンス時間が短いことにある．原子核スピンが化学結合で強く結合されている分子を使えばこの困難は解決されるが，単一分子のスピン共鳴信号が非常に小さく現在の技術では検出できない．NMR 量子コンピュータでは $O(10^{18})$ 個の分子のバルクアンサンブルによる「実効的純粋状態」を作り出すことによってこれを解決し，簡単な量子アルゴリズムを実験室で実証した．しかし初期状態の分極ができないために，信号強度が q ビット個数の指数関数で減衰するという犠牲を払わなければならず，その能力は制約を受ける．

これらの例が示すように，量子コンピュータに対して良い物理的実現法を見つけることはトレードオフを伴う手際を要する仕事である．上の方法はすべて不満足なものであり，これを使って近い将来に大規模量子コンピュータを実現することは誰にもできないであろう．しかしそれは可能性を排除するものではなく，他にも多くの方法が実際に提案されている．この最後の項ではそれらの幾つかを簡単に紹介する．

実現方法の分類法は q ビット表現に用いる物理的自由度によるのがよい．図 7.1 を思い出すと量子ユニットとして重要なのは q ビットであるが，これまでに見てきたように光子やスピンのような基本的粒子は特に良い選択である．

q ビット表現として使えるもう 1 つの基本的量子ユニットは**電荷**である．現代のエレクトロニクスは単一電子レベルにおいて電荷を発生し，制御し，測定する非常に優れた技術を持っている．例えば，半導体材料，金属，あるいは小さな分子から作られた**量子ドット**は荷電量子を閉じ込める静電ポテンシャルを持った 3 次元の箱として使える．これは Coulomb ブロッケード効果の観測によって実証されており，この効果では電子 1 個を追加するに要するエネルギーが $e^2/2C$ であることを反映して，静電容量 $C$ を有する量子ドットを通る電気伝導度が量子ドットにかかる電圧の関数として離散的なステップで増加する．光子と違って（正味の）電荷は壊れることがなく，動き回るだけなので電荷の状態 q ビットは 7.4.2 項の 2 重軌道表現のようなものを用いなければならないであろう．つまり $|0\rangle$ 状態と $|1\rangle$ 状態を 2 つの量子ドットのいずれかに存在する電荷に対応させるか，あるいは単一量子ドット内の 2 つの状態に対応させる．

単一光子の場合と同様に，荷電状態 q ビットへの単一 q ビット演算は（光位相シフタと類似の）静電ゲートと，電子を動かすための単一モード導波路結合器（ビー

ムスプリッタに類似）または量子ドットのためのトンネル接合のいずれかを用いて実行できる．電荷は他の電荷から長距離 Coulomb 相互作用を受け（距離 $r$ において単一電荷が作るポテンシャルは $V(r) = e/4\pi\epsilon r$），したがって離れたところにある電荷でも，ちょうど光子間の Kerr 相互作用と同じく局所的電荷の位相を変調することができる．したがって制御 Coulomb 相互作用を用いて 2 個の q ビット演算を行うことができる．最後に単一電子の電荷は直接測定できる．現代の電界効果トランジスタはそのチャンネルにある単一電荷の動きを容易に測定でき，$\approx 100$ ミリケルビンの温度で動作する単一電子トランジスタは 200 MHz 以上の周波数において $10^{-4}e/\sqrt{Hz}$ より高感度で電荷を検出できる．残念ながら制御できない遠方の電荷によって位相の乱れが生じる．これとフォノン相互作用のような散乱機構によって電荷のコヒーレンス時間が短くなり，数百フェムト秒から数百ピコ秒の桁になる．

超伝導体中の荷電キャリアも q ビット表現として示唆されている．ある種の金属では 2 個の電子がフォノン相互作用を通じて相互に束縛して電荷 $2e$ を持つ Cooper 対を形成する．電子を量子ドットに閉じ込めるのと同様に，閉じ込められた Cooper 対の数が良い量子数となるように，Cooper 対を静電的箱に閉じ込めて量子情報の表現に用いる．単一 q ビット演算は箱のポテンシャルを変調するための静電ゲートと，結合された箱の間の Josephson 接合を使って実現できる．これらの接合は q ビットを結合するのにも用いられ，超伝導干渉ループと適切に結合することにより，外部磁界を使ってその強さを変調できる．最後に q ビット測定には単に電荷測定を用いればよい．この超伝導 q ビット表現は Cooper 対が比較的ロバストなので興味深い．推定によれば主なコヒーレンスの劣化要因は電磁気的な光子の自然放出であり，1 マイクロ秒を越すコヒーレンス時間が許される．これは典型的な動的時間スケールである数百ピコ秒に比べると非常に長い．不幸なことに電荷表現の場合と同様に，無関係な電荷（「準粒子」(quasiparticle)）の背景が変動するのが，q ビットのコヒーレンスに非常に有害である．超伝導技術を用いてこの問題を回避する別の方法は，**磁束**(magnetic flux) を用いて q ビットを表現することであり，ここでは超伝導ループ素子に局所化された右手系と左手系の向きの磁束が q ビット状態に対応する．このコヒーレンス劣化は背景の磁気的変動によって生じ，静電的な場合よりはるかに静かであると期待されている．

磁気的相互作用の局所性は q ビット表現にとって都合の良い性質なので再びス

ピンに戻ると，スピンに対して固体技術を利用する方法が提案されている．多くの電子を含むかなり大きな量子ドットで，スピンが 1 個余計な電子で担われていると，これはスピン 1/2 の物体として振る舞う．このスピン状態は低温の強い磁界中で熱平衡において，スピン反転エネルギーを $k_{\mathrm{B}}T$ よりも十分大きくすることによって作られる．7.7 節で見たように単一スピンの操作は局所的パルス磁界を加えて行い，結合した q ビット演算は制御した Heisenberg 結合：

$$H(t) = J(t)\vec{S}_1 \cdot \vec{S}_2 = \frac{1}{4}\left[X_1X_2 + Y_1Y_2 + Z_1Z_2\right] \tag{7.174}$$

により実現できる．ここで $\vec{S}$ はスピンオペレータ（Pauli のオペレータを 2 で割ったもの），$J(t) = 4\tau_0^2(t)/u$，$u$ はドットの帯電エネルギー，$\tau_0(t)$ はドット間に置かれた局所的静電ゲートにより制御されたトンネル行列要素である．この相互作用は制御 NOT と等価であるという意味で普遍的である（下の演習 7.52 参照）．理論上スピン状態はスピンを運ぶ電子を読み出し常磁性ドットにトンネルさせるか，「スピンバルブ」を通してスピンに依存したトンネルを起こさせて電位計で読み取る．困難な点はそのような測定を実際に行うことであり，現在の技術で半導体中の高忠実度な単一スピン測定は実現されていない．

**演習 7.52:（Heisenberg Hamiltonian の普遍性）**　交換演算 $U$ は Heisenberg 結合 Hamiltonian (7.174) 中の $J(t)$ を適切な時間加えて，$U = \exp(-i\pi\vec{S}_1\cdot\vec{S}_2)$ とすることによって実現できることを示せ．この半分の時間の相互作用を加えて得られる「$\sqrt{\mathrm{SWAP}}$」ゲートは普遍的である．この変換を計算し，それを単一 q ビット演算で構成することにより制御 NOT を得る方法を示せ．

最終的には十分進歩した技術によって半導体中に単一核スピンを配置し，制御し，測定することが可能となって，次のような夢を実現できるかも知れない．単一の燐原子（核スピン 1/2）を $^{28}$Si 結晶ウエハ（核スピン 0）上にリソグラフィでパターン化した静電ゲートの下に正確に置くと想像する．このゲートは $^{31}$P 不純物周辺の電子雲を操作して $^{31}$P 原子核から見た磁界を変調することにより単一 q ビット演算を実行する．$^{31}$P 不純物を分離する領域の上に設けた別の電極により，隣接した $^{31}$P を化学結合のように結び付ける電子分布を作り出す．このよう

にして 2 - q ビット演算が実行できる．このような方法の製作上の制約には難しいものがある — 例えばゲート間隔は 100Å またはそれ以下であり，$^{31}$P 不純物を正確に規則的配列で配置しなければならない．けれどもこのビジョンは少なくとも量子計算を従来の計算技術と結び付けるために可能な研究領域を明瞭に表現している．

量子コンピュータを実現するために述べてきた方法の中で，技術者の注意を最も引き付けるのは固体技術に基づくものである．もちろん原子，分子，および光学的な量子計算法も，この分野の最先端である光格子 (optical lattice)（交差した光ビームに閉じ込められた原子で構成される人工的な結晶）や Bose 凝縮 (Bose condensation) のようなシステムを用いて提案されるし，何時の日か中間子，クォーク，グルオン，またはブラックホールさえ使った量子計算が提案されるかも知れない．しかし**何らかの**種類の固体量子コンピュータを想像する動機は非常に大きい．1940 年代後半にトランジスタが発明されて以来，世界中で 1 兆 US ドル以上がシリコン技術に投資がされてきたと推定される．固体システムはまた超伝導，量子 Hall 効果，Coulomn ブロッケード（これは古典物理学に関することはすべてよくわかっていると，広く久しく信じられてきた後で発見された古典的効果である！）のような新たな物理学を豊かに育んできた．

本章は主として量子計算機械の実現に重きを置いてきたが，ここに述べた基本的概念は多くの他の量子的応用にも有用である．量子暗号とその実験的な実現方法は 12.6 節（第 III 巻）で述べる．量子テレポーテーションや超高密度符号化に関する実験的研究に関しては章末の「歴史と参考資料」欄に示唆が与えられている．量子通信と計算の一般的境界には分散量子計算のような挑戦的課題があり，そのようなシステムの新しいアルゴリズムと実験的な実現法の開発は，確実に将来の豊かな研究分野となるであろう．

量子計算と量子情報機械の魅力の大部分は，確かに新たな情報技術のようなその潜在的な経済効果である．しかし本章で見たように，量子計算と量子情報は物理システムに関する新たな疑問を提起し，その性質を理解するための別の方法を提供する．この新しいアイディアは，原子から凝縮物質システムにいたるすべての伝統的な物理システムの多体問題・統計・熱力学等の研究から，離れる必要性を具体的に表現している．それに代わって**単一**量子レベルにおける物理システムの**ダイナミック**な性質に焦点を当てる新たな機会を示している．この豊かなアプロー

チの香りを示すことにより，読者にとって本章が物理学に関して「アルゴリズム的に考え」続ける動機となれば幸いである．

**問題 7.1:（効率的な時間ラベル）** $2^n \times 2^n$ 対角密度行列で，$|0^n\rangle\langle 0^n|$ を除いてすべての対角要素を循環的に置換する，効率的な（$O(\text{poly}(n))$ 個のゲートしか必要としない）回路を構築できるか？

**問題 7.2:（線形光学による計算）** 単一光子で量子計算を行うに際して 7.4.1 項の 2 重軌道表現に代わって，**単項**(unary) 状態表現を使う．つまり $|00\ldots01\rangle$ は 0，$|00\ldots010\rangle$ は 1，$|00\ldots0100\rangle$ は 2 等々で $|10\ldots0\rangle$ は $2^n-1$ である．

(1) これらの状態に対する任意のユニタリー変換はビームスプリッタと位相シフタだけで (非線形媒質を使わずに) 完全に構成できることを示せ．

(2) 1 - q ビットの Deutsch-Jozsa アルゴリズムを実行するためのビームスプリッタと位相シフタの回路を示せ．

(3) 2 - q ビットの量子探索アルゴリズムを実行するためのビームスプリッタと位相シフタの回路を示せ．

(4) 任意のユニタリー変換を実現するには一般に（$n$ の）指数関数的数の部品を必要とすることを証明せよ．

**問題 7.3:（Jaynes-Cummings 相互作用を通した制御）** 小さな量子システムの — 外部の**古典的**自由度を通した — ロバストで正確な制御は量子計算能力にとって重要である．原子状態に著しいコヒーレンス劣化を生じる重ね合せを起こすことなく，光パルスを加えることで原子状態が制御できるのは注目すべきである！ この問題ではこれが起きるにはどんな近似が必要かを調べる．単一モードの電磁界と結合した単一原子に対する Jaynes-Cummings の Hamiltonian から出発する：

$$H = a^\dagger \sigma_- + a\sigma_+, \tag{7.175}$$

ここで $\sigma_\pm$ は原子に，$a, a^\dagger$ は電磁界に働く．

(1) $U = e^{i\theta H}$ に対して次式を計算せよ．

$$A_n = \langle n|U|\alpha\rangle, \tag{7.176}$$

ここで，$|\alpha\rangle$ と $|n\rangle$ はそれぞれ電磁界のコヒーレント状態と光子数固有状態である．$A_n$ は原子状態に働く**オペレータ**である．次式を求めよ．

$$A_n = e^{-|\alpha^2|}\frac{|\alpha|^2}{n!}\begin{bmatrix} \cos(\theta\sqrt{n}) & \frac{i\sqrt{n}}{\alpha}\sin(\theta\sqrt{n}) \\ \frac{i\alpha}{\sqrt{n+1}}\sin(\theta\sqrt{n+1}) & \cos(\theta\sqrt{n+1}) \end{bmatrix} \tag{7.177}$$

演習 7.17 の結果が役に立つ．

(2) $\alpha$ が大きい近似をすると便利である（$\alpha$ を実数としても一般性を失わない）．確率分布：

$$p_n = e^{-x}\frac{x^n}{n!} \tag{7.178}$$

を考える．このとき平均値は $\langle n\rangle = x$, 標準偏差は $\sqrt{\langle n^2\rangle - \langle n\rangle^2} = \sqrt{x}$ である．変数を変換し $n = x - L\sqrt{x}$，Stirling の近似：

$$n! \approx \sqrt{2\pi n}\; n^n e^{-n} \tag{7.179}$$

を用いて次式を求めよ．

$$p_L \approx \frac{e^{-L^2/2}}{\sqrt{2\pi}}. \tag{7.180}$$

(3) $n = |\alpha|^2$ に対して最も重要な項は $A_n$ である．$n = \alpha^2 + L\alpha$ を定義し，

$$a = y\sqrt{\frac{1}{y^2}+\frac{L}{y}} \quad \text{および} \quad b = y\sqrt{\frac{1}{y^2}+\frac{L}{y}+1},$$
$$\text{ただし } y = 1/\alpha \tag{7.181}$$

に対して，$\theta = \varphi/\alpha$ を用いて

$$A_L \approx \frac{e^{-L^2/4}}{(2\pi)^{1/4}}\begin{bmatrix} \cos a\varphi & ia\sin a\varphi \\ (i/b)\sin b\varphi & \cos b\varphi \end{bmatrix} \tag{7.182}$$

を示せ．また期待される通りに次式が成り立つことを証明せよ．

$$\int_{-\infty}^{\infty} A_L^\dagger A_L dL = I. \tag{7.183}$$

(4) 原子に生じる理想的ユニタリー変換は

$$U = \begin{bmatrix} \cos\alpha\theta & i\sin\alpha\theta \\ i\sin\alpha\theta & \cos\alpha\theta \end{bmatrix} \tag{7.184}$$

である．$A_L$ は $U$ にどれくらい近いか？ **忠実度**：

$$\mathcal{F} = \min_{|\varphi\rangle} \int_{-\infty}^{\infty} |\langle\psi|U^\dagger A_L|\psi\rangle|^2 dL \tag{7.185}$$

を $y$ の Taylor 級数として推定できれば試みよ．

**問題 7.4:（2準位原子によるイオントラップ論理）** 7.6.3項で述べた制御NOTゲートは簡単のために3準位原子を用いた．少し複雑になるがこの問題に示すように第3の準位なしでも行うことができる．

$\Upsilon_{\hat{n}}^{\mathrm{blue},j}(\theta)$ は $j$ 番目の粒子に時間 $\theta\sqrt{N}/\eta\Omega$ の間，青色側帯波 $\omega = \Omega + \omega_z$ の光パルスを加えて達成できる演算を表すとし，赤色側帯波に対しても同様とする．$\hat{n}$ は入射光の位相設定で制御された $\hat{x}$ - $\hat{y}$ 平面内の回転軸を表す．どのイオンに適用するかが明確なときは上添字 $j$ を省略してもよい．具体的に言うと

$$\Upsilon_{\hat{n}}^{\mathrm{blue},j}(\theta) = \exp\left[\left(e^{i\varphi}|00\rangle\langle 11| + e^{-i\varphi}|11\rangle\langle 00| + e^{i\varphi}\sqrt{2}|01\rangle\langle 12| + e^{-i\varphi}\sqrt{2}|12\rangle\langle 01| + \cdots\right)\frac{i\theta}{2}\right], \tag{7.186}$$

ここで $\hat{n} = \hat{x}\cos\varphi + \hat{y}\sin\varphi$，ケット中の2つの記号は左から右へ内部状態と運動状態を表現する．因子 $\sqrt{2}$ はボソン状態に対して $a^\dagger|n\rangle = \sqrt{n+1}|n+1\rangle$ という事実から生じる．

(1) $S^j = \Upsilon_{\hat{n}}^{\mathrm{red},j}(\pi)$ は運動状態が最初 $|0\rangle$ のときに，イオン $j$ の内部状態と運動状態の間の交換を実行することを示せ．

(2) $|00\rangle$，$|01\rangle$，$|10\rangle$，$|11\rangle$ が張る計算部分空間における任意の状態に働く $\Upsilon_{\hat{n}}^{\mathrm{blue},j}(\theta)$ が，その状態を同じ部分空間に変換するような $\theta$ の値を求めよ．これは任意の軸 $\hat{n}$ に対して成立しなければならない．

(3) $\Upsilon_{\hat{n}}^{\mathrm{blue},j}(\varphi)$ が計算部分空間内に留まるならば，任意に選んだ回転角 $\beta$ と軸 $\alpha$ に対して，$U \equiv \Upsilon_{\alpha}^{\mathrm{blue}}(-\beta)\Upsilon_{\hat{n}}^{\mathrm{blue}}(\theta)\Upsilon_{\alpha}^{\mathrm{blue}}(\beta)$ も同じ計算部分空間内に留まることを示せ．

(4) $U$ が対角となるような $\alpha$ と $\beta$ を見出せ．具体的には

$$\begin{bmatrix} e^{-i\pi/\sqrt{2}} & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\pi/\sqrt{2}} \end{bmatrix} \tag{7.187}$$

のようなオペレータを見つけると役に立つ．

(5) 式 (7.187) は単一 q ビット演算と共に，2 個のイオンの内部状態間の制御 NOT ゲートを構成できる有意なゲートを記述することを示せ．運動状態を $|0\rangle$ に初期化することなく，制御 NOT を実行するための合成パルス列を見い出せるか？

## 第 7 章のまとめ: 量子コンピュータ：物理的実現法

- **4 つの基本的要請**　量子計算の実行には 4 つの基本的要請がある：
  (1) q ビットの表現
  (2) 制御可能なユニタリー時間発展
  (3) 初期 q ビット状態の作成
  (4) 最終 q ビット状態の測定
- **単一光子**　状態 $|01\rangle$, $|10\rangle$ を論理的 0 と 1 に用いると，単一光子は良い q ビットとして使える．しかし，単一光子の相互作用を起こすほど強い従来の非線形光学材料では，光子の散乱または吸収が避けられない．
- **共振器 QED**　単一原子が単一光子と強く相互作用できる技術である．原子を用いて単一光子間の相互作用を仲介する機構を提供する．
- **トラップイオン**　イオンの電子スピンおよび核スピン状態をレーザパルスの照射で制御できるまで，イオンを閉じ込めて冷却できる．スピン状態を質量中心フォノンに結合すると，異なるイオン間の論理ゲートが実行できる．
- **核スピン**　核スピンは理想に近い q ビットであり，スピン状態の制御と測定ができさえすれば単一分子は理想に近い量子コンピュータになり

得る．室温で分子の大きなアンサンブルを使い核磁気共鳴によってこれが可能であるが，初期化手続きが十分でないので信号損失が大きい．

## 歴史と参考資料

量子コンピュータを作るのがなぜ難しいかの優れた議論はDiVincenzo [DiV95a]の論文を見て欲しい．図7.1はこれに基づいている．DiVincenzoはまた量子コンピュータを実現するための5つの基準を示しており，それは7.2節で議論したものと似ている．

7.3節の量子単純調和振動子は量子力学の主要課題であり，[Sak95]をはじめどの標準的な教科書でも扱っている．7.3.3項で述べた量子コンピュータに必要かつ十分な一般的条件はLloyd [Llo94]により議論された．

7.4節の光学的量子コンピュータは主要な理論ツールとして量子光学の形式を使っており，これは多くの教科書に述べられている．優れたものを2つあげると[Lou73] [Gar91]がある．偏光子，ビームスプリッタ，光子検出器等々のような基礎光学と光技術に対しては例えば教科書[ST91]がある．単一光子領域のビームスプリッタはCampos, Saleh, Tiechにより研究され[CST89]，それと関連して$SU(2)$と2つの調和振動子の簡潔な関係がSchwingerにより最初に述べられた[Sak95]．qビットの「2重軌道」表現の概念はYurkeにより示され，（非線形Kerr媒質を使った）完全な量子コンピュータを記述して，（演習7.13のような）Deutsch-Jozsaのアルゴリズムを実行するために，ChuangとYamamotoにより用いられた[CY95]．量子光学的FredkinゲートはYamamoto, Kitagawa, Igeta [YKI88]およびMilburn [Mil89a]により最初に述べられた．光学的量子コンピュータに要求される単一光子発生と検出技術はImamogluとYamamoto [IY94]，Kwiat, Steinberg, Chiao, Eberland, Petroff [KSC+94]により議論されている．Kerr効果相互作用に代わって電子光学とCoulomb相互作用を用いた同様の機構がKitagawaとUeda [KU91]により議論された．単一量子レベルの従来の非共鳴非線形光学材料の基本的限界はWatanabeとYamamotoにより研究された[WY90]．Cerf, Adami, Kwiatは（指数関数的に多数の）線形光

学部品を使った量子論理のシミュレーションを研究した [CAK98]．影響力の強い Reck, Zeilinger, Bernstein, Bertani の初期の論文 [RZBB94] も同様の構成を述べているが，量子計算との明示的な関係は与えていない．Kwiat, Mitchel, Schwindt, White は線形光学系を用いて Grover の量子探索アルゴリズムの光学的シミュレーション系を構成したが，拡張するには指数関数的リソースを必要とする [KMSW99]．異なる距離の光通信のエネルギー論に関する議論は Miller [Mil89b] を参照．

Allen と Eberly は 2 準位原子と光共鳴に関する簡潔な取り扱いを示した [AE75]．7.5.4 項で述べた実験は Caltech の Turchette, Hood, Lange, Mabuchi, Kimble によって 1995 年に行われた [THL+95]．詳細な説明は Turchette の博士論文 [Tur97] にも述べられている．この実験の用いられた光子は「空飛ぶ q ビット」(flying qubit) と呼ばれた．原子状態を q ビットとして用い，原子が光共振器を横切る異なるアプローチが Domokos, Raimond, Brune, Haroche [DRBH95] によって提案されている．これは単一原子を用いて共振器中でコヒーレント状態をスイッチするアイディアに基づいており，Dividovich, Maali, Brune, Raimond, Haroche [DRBH87] [DMB+93] に述べられている．

イオントラップ量子計算のアイディアは Cirac と Zoller により提案された [CZ95]．このアイディアに関する 7.6.1 項の議論は Steane [Ste97] と Wineland, Monroe, Itano, Leibfried, King, Meekof [WMI+98] に負うところが大きい．Earnshaw の定理は彼の原論文にあるように [Ear42] Laplace の方程式から得られ，Ramo, Whinnery, van Duzer [RWvD84] のような現代の電磁気学の教科書にも出ている．図 7.8 は [Ste97] の図 6 にならっており，図 7.7 は [WMI+98] による．7.6.4 項の実験は Colorado 州 Boulder の National Institute of Standards and Teechnology の Monroe, Meekof, King, Itano, Wineland によって行われた [MMK+95]．図 7.15 は Wineland [WMI+98] の厚意により掲載した．Brewer, DeVoe, Kallenbach は拡張可能な量子コンピュータとして平面状のイオンマイクロトラップの大規模な配列を考えた [BDK92]．これは図 7.12 に示した種類のトラップである．James はイオントラップにおける加熱やその他コヒーレンス劣化機構の一般的理論を展開した [Jam98]．Plenio と Knight もイオントラップ量子計算におけるコヒーレンス劣化の影響を深く研究し 2 準位近似の破綻の効果も考察した [PK96].

DiVincenzo が核スピンを量子計算に用いることを最初に示唆し [DiV95b]，よく知られた古い技術である ENDOR (electron nucleon double resonance) パルス列が本質的に制御 NOT の事例であることを指摘した．しかし，量子計算のために室温で原子核アンサンブルをどう使うかという問題を解決したのは Cory, Fahmy, Havel [CFH97] であり，Gershenfeld, Chuang [GC97] は実効的純粋状態が作成できることを示した．量子アルゴリズムを修正してアンサンブル読み出しができるようにする必要があったが，この問題は [GC97] で提唱され 7.7.3 項で述べられている．NMR に関する優れた教科書が Ernst, Bodenhausen, Wokaun [EBW87]，および Slichter [Sli96] により書かれている．Warren は NMR 量子計算に対する批判を書いており [War97]，興味深いのは同じ論文で彼は量子計算をするのに電子スピン共鳴（ESR）を用いることを提唱している．時間ラベルは Knill, Chuang, Laflamme によって提案された [KCL98]．7.7.4 項の NMR 論理ゲート，および Bell 状態の作成回路は Chuang, Gershenfeld, Kubinec, Leung [CGKL98] により論じられた．7.7.4 項の Grover のアルゴリズムの実現法は Chuang, Gershenfeld, Kubinec [CGK98] によるもので，図 7.20 はこの論文から引用した．Linden, Kupce, Freeman は交換ゲートが NMR に対する量子計算の有効な貢献になり得ることを示し，そのためのパルス系列を準備した [LKF99]．論理ラベルを示す図 7.18 の 3 個のスピンのデータは Vandersypen, Yannoni, Sherwood, Chuang [VYSC99] による．Yamaguchi と Yamamoto は NMR の概念を結晶格子に拡大した [YY99]．図 7.21 に示した分子は，(a) Chuang, Vandersypen, Zhou, Leung, Lloyd [CVZ+98], (b) Cory, Mass, Price, Knill, Laflamme, Zurek, Havel [CMP+98]，(c) Somaroo, Tseng, Havel, Laflamme, Cory [STH+99]，(d) Vandersypen, Yannoni, Sherwood, Chuang [VYSC99]，(e) Nielsen, Knill, Laflamme [NKL98]，(f) Leung, Vandersypen, Zhou, Sherwood, Yannoni, Kubinec, Chuang [LVZ+99] による．Jones, Mosca, Hansen も小さな分子へのいろいろな量子アルゴリズムを実現している [JM98] [JMH98]．エントロピー限界を実現する最適ラベル化法は Schulman と Vazirani によって考案された [SV99].

量子情報処理への NMR アプローチに関するいろいろな批判は覆されてきた．多分最も一般的な議論は Schack と Caves [SC99] によるものであり，これは Braunstein, Caves, Jozsa, Linden, Popescu, Schack [BCJ+99] の初期の研究に基づいている．後者の主な技術上の結論は（NMR と関連はないが）Vidal と

Tarrach [Vid99], Zyczkowski, Horodecki, Sanpera, Lewenstein [ZHSL99] によっている．Linden と Popescu の議論 [LP99] も参考になる．

量子コンピュータ実現に対する提案はここにすべてを述べるにはあまりに多いので，ほんのわずかしか述べられない．ここにあげた文献における引用が別の文献への手がかりになるであろう．Lloyd は高分子システムを含む量子コンピュータの多くの実現についてのビジョンを描いた [Llo93]．Nakamura, Pashkin, Tsai は単一 Cooper 対 q ビットの制御を実証し，Rabi 振動を観測した [NPT99]．Mooij, Orlando, Levitov, Tian, van der Waal, Lloyd は超伝導磁束表現を用いた q ビット表現を研究した [MOL+99]．Patzman と Dykman は液体 He 表面の束縛電子を q ビットとして使うことを提案した [PD99]．7.8 節で述べたスピンに基づく量子ドット q ビットの実現は Loss と DiVincenzo により提案された [LD98]．演習 7.8 は彼らによる．量子ドットのコヒーレンス時間の文献への入門には Huibers, Switkes, Marcus, Campman, Gossard [HSM+98] がある．Imamoglu, Awschalom, Burkard, DiVincenzo, Loss, Sherwin, Small は共振器 QED 技術で操作された量子ドット中の電子スピンを用いて量子コンピュータを実現する提案をした [IAB+99]．シリコンベースで $^{31}$P を用いた核スピン量子コンピュータは Kane [Kan98] によって提案され，Vrijen, Yablonovitch, Wang, Jiang, Balandin, Roychowdhury, Mor, DiVincenzo はこれをシリコン・ゲルマニウムのヘテロ接合に埋め込まれた電子スピンに発展させた．最後に Brennen, Caves, Jessen, Deutsch [BCJD99] は共鳴からはるかに離れた光格子に捉えられた中性原子を使う量子計算の実行法を提案した．

量子テレポーテーションは 1 章（第 I 巻）の「歴史と参考資料」で述べたように単一光子と核スピンを q ビットとして用いて実験で実現された．この実現法の 1 つである Furusawa, Sørensen, Braunstein, Fuchs, Kimble, Polzik [FSB+98] は，（q ビットのような）量子情報の有限 Hilbert 空間表現を使うことを避けているので，本章に関連して特に注目に値する！ その代わりに彼らは（7.3.2 項で述べた位置や運動量のような）**連続変数**が量子状態を規定する無限次元 Hilbert 空間を使っている．このテレポーテーションへのアプローチは元は Vaidman [Vai94] により示唆され，Braunstein と Kimble により発展した [BK98a]．連続変数表現は Braunstein と Kimble [BK99] によって超高密度符号化に，Braunstein [Bra98] と Lloyd, Slotine [LS98] により独立に量子誤り訂正に，Lloyd, Braunstein [LB99]

によって量子計算にそれぞれ拡張された.

# 付録B　群　論

群の数学理論は量子計算と量子情報の研究において幾つかの点で有用である．5章の位数発見，素因数分解，周期発見等を一般化したアルゴリズムは**隠れ部分群問題** (hidden subgroup problem) に基づいており，10章（第III巻）の量子誤り訂正のための固定部分群 (stabilizer) の定式化は基礎的な群論に基づいている．付録Dで述べる整数論は群 $\mathbf{Z}_n^*$ の性質を用いる．そして本書全体を通じて用いる量子回路は暗にLie群の応用である．この付録Bでは群論の基本的内容を解説する．多くの基本的概念をまとめて重要な定義を示すが，群論は広大な分野なので詳細な説明は差し控える．

## B.1　基本的定義

群 $(G, \cdot)$ は群の2進数乗法演算「$\cdot$」を有する空でない集合 $G$ であり，次の性質を持つ：

- **閉じている**(closure)： すべての $g_1, g_2 \in G$ に対して $g_1 \cdot g_2 \in G$ が成立．
- **結合的である**(associative)：すべての $g_1, g_2, g_3 \in G$ に対して $(g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3)$ が成立．
- **単位元がある**(identity)： $\forall g \in G$ に対して $g \cdot e = e \cdot g = g$ が存在．
- **逆元がある**(inverse)： すべての $g \in G$ に対して $g \cdot g^{-1} = e,\ g^{-1} \cdot g = e$ を満たす $g^{-1} \in G$ が存在．

しばしば「$\cdot$」を除いて $g_1 \cdot g_2$ を簡単に $g_1 g_2$ と書く．また乗法演算を明示的に示すことなく群 $G$ を表すことがしばしばあるが，それは定義されていなければならない．

$G$ の要素の数が有限ならば群 $G$ は**有限**(finite) であるという．有限群 $G$ の**位数**(order) とは含まれる要素の数であり，$|G|$ と表す．もしすべての $g_1$，$g_2 \in G$ に対して $g_1g_2 = g_2g_1$ ならば群 $G$ は **Abel 群**(Abelian group；または可換群 commutative group) であるという．Abel 群の簡単な例は $n$ を法とする整数の加法群 $\mathbf{Z}_n$ であり，「乗法」演算つまりこの場合は剰余加法演算を有する．この演算は閉包性 (closure) と結合性 (connectivity) の公理を満たす．すべての $x$ に対して $x + 0 = x \pmod n$ なので単位元 0 が存在する．$x + (n - x) = 0 \pmod n$ なのですべての $x \in G$ は逆元 $n - x$ を有する．

要素 $g \in G$ の**位数**(order) は（$g$ をそれ自身と $r$ 回乗じた）$g^r$ が単位元要素 $e$ に等しくなるような，最小の正の整数 $r$ である．

$G$ の**部分群**(subgroup)$H$ は $G$ と同じ乗法演算のもとで，群を形成する $G$ の部分集合である．

**定理 B.1:（Lagrange の定理）** もし $H$ が有限群 $G$ の部分群ならば $|H|$ は $|G|$ を整除する．

**演習 B.1:** 有限群の任意の要素 $g$ に対して $g^r = e$ を満たす正の整数 $r$ が常に存在することを証明せよ．つまり，そのような群のあらゆる要素は位数を有する．

**演習 B.2:** Lagrange の定理を証明せよ．

**演習 B.3:** 要素 $g \in G$ の位数は $|G|$ を整除することを示せ．

$g_1$ と $g_2$ が $G$ の要素ならば，$g_1$ に関する $g_2$ の共役は要素 $g_1^{-1}g_2g_1$ である．もし $H$ が $G$ の部分群であって，すべての $g \in G$ に対して $g^{-1}Hg = H$ ならば，$H$ は正規部分群 (normal subgroup) である．群 $G$ の要素 $x$ の共役類 (conjugacy class) $G_x$ は $G_x \equiv \{g^{-1}xg | g \in G\}$ で定義される．

**演習 B.4:** もし $y \in G_x$ ならば $G_y = G_x$ であることを示せ．

**演習 B.5:** もし $x$ が Abel 群 $G$ の要素ならば $G_x = \{x\}$ であることを示せ．

Abel 群以外で興味がある群は，$n$ 個の q ビットに働く **Pauli 群**(Pauli group) である．単一 q ビットに対して Pauli 群はすべての Pauli 行列より成ると定義さ

れ，定義によって係数因子 $\pm 1$, $\pm i$ を有する：

$$G_1 \equiv \{\pm I,\ \pm iI,\ \pm X,\ \pm iX,\ \pm Y,\ \pm iY,\ \pm Z,\ \pm iZ\}. \tag{B.1}$$

この行列の集合は行列積演算のもとで群を形成する．なぜ係数因子 $\pm 1$, $\pm i$ を省かないのか訝るかも知れないが，これらを含める理由は $G_1$ が乗算のもとで閉じた合法的な群を形成できるようにするためである．一般に $n$ 個の q ビットに働く Pauli 群は Pauli 行列の $n$ 重テンソル積で構成されるものと定義され，やはり係数因子 $\pm 1$, $\pm i$ を含める．

### B.1.1 生成元

対象とする群に対する**群生成元** (group generator) の集合を用いると，群の研究が大いに簡単になることが多い．もし $G$ のすべての要素がリスト $g_1, \ldots, g_l$ の要素（を多分繰り返し使ったもの）の積として書けるならば，群 $G$ 中の要素の集合 $g_1, \ldots, g_l$ は群 $G$ を**生成**するといい $G = \langle g_1,\ \ldots, g_l\rangle$ と書く．例えば，$G_1$ の全要素は $X$, $Z$, $iI$ の積で書けるので $G_1 = \langle X,\ Z,\ iI\rangle$ である．他方で $G_1$ の全要素が $X$ のベキで書けるわけではないので $\langle X\rangle = \{I,\ X\}$ は $G$ の部分群である．群生成元に使う記号 $\langle\cdots\rangle$ は 2.2.5 項（第 I 巻）で述べた観測量の平均値と混同されるおそれがあるが，実際には文脈から記号の使い方を区別できる．

群を記述するのに生成元を用いる大きな利点は，これが群を**簡潔**に記述する手段となることである．$G$ はサイズ $|G|$ を有するとする．このとき $G$ を生成する $\log(|G|)$ 個の生成元の集合があるのを示すことは難しくない．これを示すのに $g_1, \ldots, g_l$ は群 $G$ の要素の集合，$g$ は $\langle g_1,\ \ldots,\ g_l\rangle$ の要素でないとする．$f \in \langle g_1,\ \ldots,\ g_l\rangle$ とすると，$fg \notin \langle g_1,\ \ldots,\ g_l\rangle$．なぜなら，もしそうならば $g = f^{-1}fg \in \langle g_1,\ \ldots,\ g_l\rangle$ となり仮定に反する．したがって各要素 $f \in \langle g_1,\ \ldots,\ g_l\rangle$ に対して，$\langle g_1,\ \ldots,\ g_l,\ g\rangle$ にあるが $\langle g_1,\ \ldots,\ g_l\rangle$ にはない要素 $fg$ が存在する．したがって，$\langle g_1,\ \ldots,\ g_l\rangle$ に生成元 $g$ を加えると生成される群のサイズをほとんど 2 倍（あるいはそれ以上）に増やすことができるので，$G$ はたかだか $\log(|G|)$ 個の要素を持たねばならないと結論される．

### B.1.2　巡回群

**巡回群**(cyclic group) $G$ はその任意の要素 $g \in G$ がある整数 $n$ に対して $a^n$ として表現できる要素 $a$ を有する．$a$ を $G$ の**生成元**(generator) と呼び $G = \langle a \rangle$ と書く．$g \in G$ により生成される**巡回部分群**(cyclic subgroup) $H$ は $\{e,\ g,\ g^2,\ \ldots,\ g^{r-1}\}$ で構成される群である．ここで $r$ は $g$ の位数である．つまり $H = \langle g \rangle$ である．

**演習 B.6:** 素数の位数を持つ任意の群は巡回的であることを示せ.

**演習 B.7:** 巡回群の部分群はすべて巡回群であることを示せ.

**演習 B.8:** もし $g \in G$ が有限の位数 $r$ を持つならば，$m = n \pmod r$ のときにのみ $g^m = g^n$ であることを示せ.

### B.1.3　剰余類

$G$ の部分群 $H$ に対して $g \in G$ で決定される $G$ 中の $H$ の**左剰余類**(left coset) は集合 $gH \equiv \{gh | h \in H\}$ である．右剰余類も同様に定義される．剰余類が「左」剰余類であるか「右」剰余類であるかは文脈で示されることが多い．群の演算が加法である群 $\mathbf{Z}_n$ の場合，部分群 $H$ の剰余類を $g \in \mathbf{Z}_n$ に対して $g + H$ と書くのが慣用である．剰余類 $gH$ の特定の要素をその剰余類の**剰余類表現**(coset representation) と呼ぶ.

**演習 B.9:** 剰余類は要素間の等価関係を定義する．$g_1,\ g_2 \in G$ が $G$ の中の $H$ と同じ剰余類の中にあるのは，$g_2 = g_1 h$ なる $h \in G$ が存在するときだけであることを示せ.

**演習 B.10:** $G$ には $H$ の剰余類が幾つ存在するか？

## B.2　表　現

$M_n$ は $n \times n$ の複素数行列の集合であるとする．行列の群とは行列積のもとで群の性質を満たす $M_n$ の中の行列の集合である．そのような群の単位要素を $I$ と

表す．群 $G$ の**表現**(representation) $\rho$ は群の乗法を保って $G$ を行列群に写像する関数として定義する．具体的には $g \in G$ が $\rho(g) \in M_n$ に写像されると，これは $g_1 g_2 = g_3$ は $\rho(g_1)\rho(g_2) = \rho(g_3)$ を意味する．もし多対 1 の写像ならばその写像は**準同形**(homomorphism) であるという．もし 1 対 1 の写像ならばその写像は**同形**(isomorphism) であるという．$M_n$ に写像される表現 $\rho$ は**次元**(dimension) $d_\rho = n$ を有する．我々が定義した表現を**行列表現**(matrix representation) とも呼ぶ．これよりも一般的なものもあるが，我々の目的にはこれで十分である．以後この付録で扱う群 $G$ は有限群とする．

### B.2.1 等価と可約

表現に関する 2 つの重要な概念は**等価**(同値，equivalence) と**可約** (縮約可能，reducibility) である．行列群 $G \subset M_n$ の**指標**(character) とは $g \in G$ に対して $\chi(g) = \mathrm{tr}(g)$ で定義される群の関数である．ここで $\mathrm{tr}(\cdot)$ は通常の行列に対するトレース関数である．指標は次の性質を持つ：

(1) $\chi(I) = n$

(2) $|\chi(g)| \le n$

(3) $|\chi(g)| = n$ は $g = e^{i\theta} I$ を意味する．

(4) $\chi$ は $G$ の任意の与えられた共役類 (conjugacy class) 上で一定である．

(5) $\chi(g^{-1}) = \chi^*(g)$

(6) $\chi(g)$ はすべての $g$ に対して代数的な数である．

2 つの行列群が同形であるときそれらは**等価**(同値，equivalent) であるといい，同形のもとで対応する要素は同じ指標を持つ．

**演習 B.11:（指標）** 上に述べた指標の性質を証明せよ．

**演習 B.12:（ユニタリー行列群）** ユニタリー行列群は（$U^\dagger U = I$ を満たす）ユニタリー行列のみで構成される．あらゆる行列群はユニタリー行列群と等価であることを示せ．もし群の表現がユニタリー行列だけから成るならば，それを**ユニタリー表現** (unitary representation) と呼ぶ．

$M_n$ の行列群 $G$ がブロック対角形の別の行列群 $H$ と等価であるならば，$G$ は**完全可約** (completely reducible) であるという．ここでブロック対角形とはある $m_1 \in M_{n_1}$，$m_2 \in M_{n_2}$ に対してすべての要素 $m \in H$ が $\mathrm{diag}(m_1, m_2)$ の形であることをいう．もしそのような等価関係が存在しないならば，行列群は既約 (irreducible) であるという．既約行列群の便利な性質を次に示す：

**補題 B.2:** **（Schur の補題）** $G \subset M_n$ と $H \subset M_k$ は同じ位数を持つ 2 つの行列群 $|G| = |H|$ であるとする．すべての要素 $g_i \in G$，$h_i \in H$ のある配列に対して $Sg_i = h_iS$ となるような $k \times n$ 行列 $S$ が存在するならば，$S$ はゼロ行列であるか，または $n = k$ であって $S$ は非特異 (nonsingular) な正方行列である．

**演習 B.13:** あらゆる既約 Abel 行列群は 1 次元であることを示せ．

**演習 B.14:** もし $\rho$ が $G$ の既約表現ならば $|G|/d_\rho$ は整数であることを証明せよ．

次の定理は既約性と指標とを関係付ける：

**定理 B.3:** 行列群 $G$ が既約であるのは次の場合に限る．

$$\frac{1}{|G|} \sum_{g \in G} |\chi(g)|^2 = 1. \tag{B.2}$$

## B.2.2　直交性

表現論の鍵となるのは次の定理である：

**定理 B.4:** **（基本定理）** あらゆる群 $G$ は正確に $r$ 個の非同値 (非等価，inequivalent)・既約 (irreducible) の表現を有する．ここで $r$ は $G$ の共役類の数である．またもし $\rho^p \in M_{d_\rho}$ と $\rho^q$ がこれらの任意の 2 つならば，行列要素は次の直交関係を満たす：

$$\sum_{g \in G} \left[\rho^p(g)\right]^{-1}_{ij} \left[\rho^q(g)\right]_{kl} = \frac{|G|}{d_\rho} \delta_{il} \delta_{jk} \delta_{pq}, \tag{B.3}$$

ここで $\rho^p = \rho^q$ ならば $\delta_{pq} = 1$，そうでなければ 0 である．

**演習 B.15:** 基本定理を用いて指標は直交することを証明せよ．つまり

$$\sum_{i=1}^{r} r_i (\chi_i^p)^* \chi_i^q = |G|\delta_{pq} \quad \text{および} \quad \sum_{p=1}^{r} (\chi_i^p)^* \chi_j^p = \frac{|G|}{r_i}\delta_{ij}, \tag{B.4}$$

ここで $p$, $q$, $\delta_{pq}$ は定理と同じ意味を持ち，$\chi_i^p$ は $G$ の $i$ 番目の共役類上で $p$ 番目の既約表現の指標がとる値，$r_i$ は $i$ 番目の共役類の大きさである．

**演習 B.16:** $S_3$ は 3 つの要素の置換群 (permutation group) である．これを 123 から 123; 231; 312; 213; 132; 321 への写像として並べるとする．$S_3$ には 2 つの 1 次元既約表現が存在し，その一方は自明であるが他方は上記の置換の順序に対応して 1, 1, 1, −1, −1, −1 であることを示せ．また行列

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \frac{1}{2}\begin{bmatrix} -1 & -\sqrt{3} \\ \sqrt{3} & -1 \end{bmatrix}, \quad \frac{1}{2}\begin{bmatrix} -1 & \sqrt{3} \\ -\sqrt{3} & -1 \end{bmatrix},$$

$$\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \frac{1}{2}\begin{bmatrix} 1 & \sqrt{3} \\ \sqrt{3} & -1 \end{bmatrix}, \quad \frac{1}{2}\begin{bmatrix} 1 & -\sqrt{3} \\ -\sqrt{3} & -1 \end{bmatrix}, \tag{B.5}$$

を有する 2 次元既約表現が存在することを示せ．この表現が直交することを証明せよ．

## B.2.3 正則表現

数 1 は任意の群の正当な 1 次元行列表現であるが，それは自明である．もし表現の行列群が元の群に対して同形 (isomorphic) ならば，その表現は**忠実**(faithful) であるという．**正則表現**(regular representation) は任意の群に存在する忠実な表現であり，次のようにして構築できる．$\vec{v} = [g_1, g_2, \ldots, g_{|G|}]^T$ は $G$ の要素の列ベクトルである．$\vec{v}$ の各要素に要素 $g \in G$ を掛けるとベクトル要素が並べ換わる．この並べ換えは $\vec{v}$ に行列積として働く $|G| \times |G|$ 行列で表現される．異なる可能な並べ換えに対応するそのような $|G|$ 個の行列は，行列積のもとで $G$ の忠実な表現を形成する．

**演習 B.17:** 正則表現は忠実であることを証明せよ．

**演習 B.18:** 単位元の表現以外の正則表現の指標はゼロであり，単位元の表現に対して $\chi(I) = |G|$ であることを示せ．

任意の表現を既約表現のテンソル和に分解するすることに関して，次の定理が成り立つ．

**定理 B.5:** もし $\rho$ が指標 $\chi$ を有する $G$ の任意の表現であり，$\rho^p$ が指標 $\chi^p$ を有する $G$ の非同値な既約表現ならば，$\rho = \bigoplus_p c_p \rho^p$ である．ここで $\bigoplus$ は直和を表し，$c_p$ は次式で決められる数である：

$$c_p = \frac{1}{|G|} \sum_{i=1}^{r} r_i (\chi_i^p)^* \chi_i. \tag{B.6}$$

**演習 B.19:** 定理 B.5 を用いて正則表現は各既約表現 $\rho^p$ の事象を $d_{\rho^p}$ 個含むことを示せ．したがって，もし $R$ が正則表現を表し，$\hat{G}$ がすべての非同値既約表現の集合を表すならば次式が成り立つ：

$$\chi_i^R = \sum_{\rho \in \hat{G}} d_\rho \chi_i^\rho. \tag{B.7}$$

**演習 B.20:** 正則表現の指標は $G$ の単位元 $e$ を含む共役類 $i$ に対する以外はゼロである．したがって次式が満たされることを示せ：

$$\sum_{\rho \in \hat{G}} d_\rho \chi^\rho(g) = N \delta_{ge}. \tag{B.8}$$

**演習 B.21:** $\sum_{\rho \in \hat{G}} d_\rho^2 = |G|$ を示せ．

## B.3　Fourier 変換

$G$ は位数 $N$ の有限群，$f$ は群の要素を複素数に写像する関数であるとする．$G$ の $d_\rho$ 次元既約表現 $\rho$ に対して，$f$ の Fourier 変換を $\hat{f}$ と定義する：

$$\hat{f}(\rho) \equiv \sqrt{\frac{d_\rho}{N}} \sum_{g \in G} f(g) \rho(g). \tag{B.9}$$

行列表現 $\rho$ に対して $\hat{f}(\rho)$ は行列から行列へ写像する．$\hat{G}$ を $G$ の非同値既約表現の完全集合とする．$\hat{f}$ の Fourier 逆変換を次のように定義する：

$$f(g) = \frac{1}{\sqrt{N}} \sum_{\rho \in \hat{G}} \sqrt{d_\rho} \mathrm{tr}(\hat{f}(\rho)\rho(g^{-1})). \tag{B.10}$$

$\sum_\rho d_\rho^2 = N$ なので $f$ と $\hat{f}$ は両方とも長さ $N$ の複素数のベクトルとして表せる．もし $\hat{G}$ がユニタリー表現より成るならば，Fourier 変換もユニタリーになるように上式の係数を選んでいることに注意する．

式 (B.9) を式 (B.10) に代入すると上の定義が理解できる：

$$\begin{aligned} f(g) &= \frac{1}{N} \sum_{\rho \in \hat{G}} \sum_{g' \in G} d_\rho \ f(g') \ \mathrm{tr}(\rho(g')\rho(g^{-1})) && \text{(B.11)} \\ &= \frac{1}{N} \sum_{\rho \in \hat{G}} \sum_{g' \in G} d_\rho \ f(g') \ \mathrm{tr}(\rho(g' g^{-1})) && \text{(B.12)} \\ &= \frac{1}{N} \sum_{g' \in G} f(g') \ \sum_{\rho \in \hat{G}} d_\rho \ \chi^\rho(g' g^{-1}). && \text{(B.13)} \end{aligned}$$

式 (B.8) を用いると式 (B.13) を希望通りに簡単化できる．

$$f(g) = \sum_{g' \in G} f(g') \ \delta_{g'g}. \tag{B.14}$$

**演習 B.22:** 式 (B.10) を式 (B.9) に代入して $\hat{f}(\rho)$ が得られることを示せ．

**演習 B.23:** 加法を群の演算として Abel 群 $G$ を $g \in [0,\ N-1]$ で表現し，$\rho_h(g) = \exp[-2\pi i g h/N]$ を $g$ の $h$ 表現であると定義する．この表現は 1 次元なので $d_\rho = 1$ である．$G$ に対する Fourier 変換の関係は

$$\hat{f}(h) = \frac{1}{\sqrt{N}} \sum_{g=0}^{N-1} \ f(g) \ e^{-2\pi i g h/N} \quad \text{および}$$

$$f(h) = \frac{1}{\sqrt{N}} \sum_{g=0}^{N-1} \ \hat{f}(g) \ e^{2\pi i h g/N} \tag{B.15}$$

であることを示せ．

**演習 B.24:** 演習 B.16 の結果を用いて $S_3$ 上の Fourier 変換を構築し，それを $6 \times 6$ のユニタリー行列で表現せよ．

## 歴史と参考資料

群論には多くの優れた教科書があり，どの代数学の書物も実質的に群論に節を割いている．ここでの議論では Lomont [Lom87] の有限群の教科書から多くの記号を借用した．Hammermesh は物理学における群論の標準的な参考書である [Ham89]．群の Fourier 変換の議論は普通はあまりない．Diaconis と Rockmore は群に関する Fourier 変換の効率的計算について良い論文を書いている [DR90]．その多くの結果は Fässler と Stiefel が解説している [FS92]．Beth [Bet84] は Clausen [Cla89] と独立に群の高速 Fourier 変換を発見した．

# 付録C　Solovay-Kitaevの定理

4 章において任意のユニタリーオペレータ $U$ は，単一 q ビットゲートと制御 NOT ゲートよりなる回路を用いた量子コンピュータ上で，実現できることを示した．このような**普遍性**の結果は，見かけ上異なる量子計算モデルの等価性を保証するので重要である．例えば，量子コンピュータのプログラマが，この普遍性の結果 4 個の入出力 q ビットを持つゲートが一定数の制御 NOT と単一 q ビットユニタリーゲートでシミュレートできることを確信して，そのゲートを含む量子回路を設計することができる．

制御 NOT と単一 q ビットユニタリーゲートの普遍性において満足できない点は，単一 q ビットゲートが**連続体**(continuum) を形成するのに対して，10 章（第 III 巻）で述べる耐故障性量子計算が**離散的**集合のゲートに対してのみ働くことである．幸い 4 章で**任意の**単一 q ビットゲートが制御 NOT，Hadamard ゲート $H$，位相ゲート $S$，および $\pi/8$ ゲートの有限のゲート集合を用いて任意の精度で近似することができることを知った．また選ばれたゲートを精度 $\epsilon$ で近似するには，この有限集合から選んだ $\Theta(1/\epsilon)$ 個のゲートしか必要としないことを発見的 (heuristic) に議論した．さらに 10 章（第 III 巻）で制御 NOT，Hadamard，位相および $\pi/8$ ゲートが耐故障性を持つ方法で実現できることを示している．

この付録では $\Theta(1/\epsilon)$ よりもずっと速い割合で収束できることを示す．**Solovay-Kitaev の定理**(Solovay-Kitaev theorem) は単一 q ビットに働く任意のゲート $U$ と与えられた任意の $\epsilon > 0$ に対して，定まった有限集合から選んだ $\Theta(\log^c(1/\epsilon))$ 個のゲートを用いて，$\epsilon$ の精度で $U$ を近似できることを示す．ここで $c$ はほぼ 2 に等しい小さい定数である．$c$ に対する最良の可能な値はまだわかっていないので，$c$ は近似的に 4 に等しいとして Solovay-Kitaev の定理を証明し，最後の問題

において $c$ を 2 の近くまで減らせる方法の概略を示す．また $c$ は 1 以下にはならないことを証明する．1 と 2 の間で可能な $c$ の最良の値を決定することは未解決な問題である！

Solovay-Kitaev の定理の重要性を知るために，$f(n)$ 個のゲートを用いて問題を解くアルゴリズムを設計する，量子コンピュータプログラマを想像する．彼もしくは彼女が見出すアルゴリズムでは，通常の耐故障性を持つ制御 NOT，Hadamard，位相および $\pi/8$ ゲートの集合以外のゲートを多数使っているとする．そのアルゴリズムを耐故障性をもって実行するには幾つのゲートが必要か？ もし全アルゴリズムに対して誤り許容度が $\epsilon$ ならば，各ゲートは $\epsilon/f(n)$ の許容度で正確でなければならない．4 章の発見的議論によればアルゴリズムに用いられる各ゲートを近似するのに，耐故障性を持つゲート $\Theta(f(n)/\epsilon)$ 個を使用すると，全コストは $\Theta(f(n))^2/\epsilon$，つまりアルゴリズムに要求されるゲート数は多項式数だけ増加する．Solovay-Kitaev の定理を用いると，アルゴリズムの各ゲートは耐故障性集合のゲート $O(\log^c(f(n)/\epsilon))$ 個でシミュレートできて，その耐故障性アルゴリズムに対する全コストは $O(f(n)\log^c(f(n)/\epsilon))$，つまり元のアルゴリズムに比べて僅か対数多項式 (polylogarithmic) 倍だけ多い数で済む．多くの問題に対してこの対数多項式数のコストは許容できるものである一方で，4 章の発見的議論で求めた多項式コストはあまり望ましくなかった．

Solovay-Kitaev の定理を正確に述べるには幾つかの記号と用語を定義する必要がある．$SU(2)$ は行列式が 1 に等しいすべての単一 q ビットユニタリー行列の集合であることを思い出そう．すべての単一 q ビットユニタリーゲートは $SU(2)$ 要素の積と重要でないグローバル位相因子で書けるので，我々は $SU(2)$ のみに注目する．$\mathcal{G}$ は $SU(2)$ 要素の有限集合であるとし，$\mathcal{G}$ が我が量子コンピュータプログラマが他のすべてのゲートをシミュレートするのに用いる基本ゲートの有限集合の役割を果たす．具体性を重んじて $\mathcal{G}$ は耐故障性集合 $H$, $S$, $T$ を含むものと考え，その行列式がすべて 1 に等しいことを保証するためにグローバル位相を含むとする．便宜上 $\mathcal{G}$ は**それ自身の逆元を含む**，つまりもし $U \in \mathcal{G}$ ならば $U^\dagger \in \mathcal{G}$ であるとする．耐故障性集合の場合にこれは集合に $S^\dagger = S^3$ と $T^\dagger = T^7$ を追加することを意味し，幸いこれらはすでに集合に含まれているゲートで記述できる．$\mathcal{G}$ から作る長さ $l$ の**語**(word) は積 $g_1 g_2 \cdots g_l \in SU(2)$ であり，ここで各 $i$ に対して $g_i \in \mathcal{G}$ である．$\mathcal{G}_l$ はたかだか長さ $l$ のすべての語の集合であり，$\langle \mathcal{G} \rangle$ は有限長

のすべての語の集合であると定義する．

ユニタリー行列を近似するという意味を定量的に表すには何か**距離**の概念が必要である．正確な尺度を用いることはそれほど重要ではない．我々の目的には，9 章で学んだ**トレース距離**(trace distance)　$D(U,\ V) \equiv \mathrm{tr}|U-V|$ を用いるのが便利である．ここで $|X| \equiv \sqrt{X^\dagger X}$ は $X^\dagger X$ の正の平方根である．実際はこの定義は 9 章（第 III 巻）で用いた定義と因子 2 だけ異なっている．異なる規格化を用いる理由はこれから見るように，Solovay-Kitaev の定理の証明を容易に幾何学的に可視化できるからである（$SU(2)$ の要素を空間の点と考えることも役に立つ）．$SU(2)$ の部分集合 $S$ が**稠密**であるとは，$SU(2)$ の任意の要素 $U$ と $\epsilon > 0$ に対して $D(s,\ U) < \epsilon$ なる要素 $s \in S$ が存在することである．$S$ と $W$ は $SU(2)$ の部分集合であるとする．このときもし $W$ のあらゆる点が $S$ のある点から距離 $\epsilon$ 以内にあるならば，$S$ は $W$ に対して $\epsilon$ **ネット**($\epsilon$-net) を形成するという．ただし $\epsilon > 0$ である．我々の興味は $l$ が増加するときに，如何に早く $\mathcal{G}_l$ が $SU(2)$ を「満たす」かにある．つまりどれだけ小さな $\epsilon$ に対して $\mathcal{G}_l$ は $SU(2)$ の $\epsilon$ ネットになるか？ である．Solovay-Kitaev の定理の述べるところは $l$ が増加すると $\epsilon$ は実際非常に早く小さくなる．

**演習 C.1:** 4 章で距離の尺度 $E(U,\ V) = \max_{|\psi\rangle} \|(U-V)|\psi\rangle\|$ を用いた．ここで最大値はすべての純粋状態 $|\psi\rangle$ に対してとる．$U$ と $V$ が単一 q ビット回転ならば，$U = R_{\hat{m}}(\theta)$，$V = R_{\hat{n}}(\varphi)$，$D(U,\ V) = 2E(U,\ V)$ であることを示し，したがって Solovay-Kitaev の定理に対してトレース距離と尺度 $E(\cdot,\ \cdot)$ のいずれを用いてもよいことを示せ．

**定理 C.1:（Solovay-Kitaev の定理）** $\mathcal{G}$ はそれ自身の逆元を含む $SU(2)$ の要素の有限集合であり，$\langle\mathcal{G}\rangle$ が $SU(2)$ で稠密であるとする．$\epsilon > 0$ が与えられたとき，$\mathcal{G}_l$ は $l = O(\log^c(1/\epsilon))$ に対して $SU(2)$ における $\epsilon$ - ネットである．ここで $c \approx 4$ である．

すでに述べたように $c$ の可能な最良の値は 4 よりなにがしか小さいが，この特定の場合に対して容易に証明できる．問題 C.1 で $c$ が小さい場合にどのように証明を変更するかを説明する．証明の最初の部分で $l$ が増加するに従い，$\mathcal{G}_l$ の点は単位行列 $I$ の小さな近傍で非常に稠密になることを示す．この結論は次の補題に

要約される．補題を述べるために，$S_\epsilon$ は $D(U,\ I) \le \epsilon$ を満たす $SU(2)$ の点 $U$ のすべての集合であると定義する．

**補題 C.2:** $\mathcal{G}$ はそれ自体の逆元を含み $\langle \mathcal{G} \rangle$ が $SU(2)$ で稠密であるような，$SU(2)$ 要素の有限集合であるとする．次の性質を持ち $\mathcal{G}$ と無関係な普遍的定数 $\epsilon_0$ が存在する：任意の $\epsilon \le \epsilon_0$ に対してもし $\mathcal{G}_l$ が $S_\epsilon$ に対する $\epsilon^2$ ネットならば，ある定数 $C$ に対して $\mathcal{G}_{5l}$ は $S_{\sqrt{C}\epsilon^{3/2}}$ に対する $C\epsilon^3$ ネットである．

我々は間もなく補題 C.2 を証明するが，その前にまずこれが Solovay-Kitaev の定理とどういう関係にあるかを見ておく．証明は 2 段階より成る．最初の段階で補題 C.2 を繰り返し適用して，語の長さ $l$ が増加すると原点の近傍が急速に満たされることを示す．$\mathcal{G}$ は $SU(2)$ において稠密なので，$\mathcal{G}_{l_0}$ が $SU(2)$ に対して，したがってまた $S_{\epsilon_0}$ に対して $\epsilon_0^2$ ネットであるような $l_0$ を見つけることができる．$\epsilon = \epsilon_0$，$l = l_0$ として補題 C.2 を適用すると，$\mathcal{G}_{5l_0}$ は $S_{\sqrt{C}\epsilon_0^{3/2}}$ に対する $C\epsilon_0^3$ ネットである．$\epsilon = \sqrt{C}\epsilon_0^{3/2}$，$l = 5l_0$ として補題 C.2 をもう一度適用すると，$\mathcal{G}_{5^2 l_0}$ は $S_{\sqrt{C}(\sqrt{C}\epsilon_0^{3/2})^{3/2}}$ に対する $C(\sqrt{C}\epsilon_0^{3/2})^3$ ネットである．この手続きを $k$ 回繰り返すと，$\mathcal{G}_{5^k l_0}$ は $S_{\epsilon(k)}$ に対する $\epsilon(k)^2$ ネットである．ここで

$$\epsilon(k) = \frac{(C\epsilon_0)^{(3/2)^k}}{C}. \tag{C.1}$$

一般性を失うことなく $C\epsilon_0 < 1$ となるように $\epsilon_0$ を選ぶと，したがって $k$ の増加によって $\epsilon(k)$ が急速に小さくなると考えてよい．また $\epsilon_0$ を十分小さく選べば $\epsilon(k)^2 < \epsilon(k+1)$ であることも使うと役に立つ．

第 2 段階は $U$ が $SU(2)$ の任意の要素であるとして，$\mathcal{G}$ の要素の積を用いて $U$ を近似する．図 C.1 に示した並進 (translation) の概念を用いて，$U_0 \in \mathcal{G}_{l_0}$ を $U$ の $\epsilon(0)^2$ 近似であるとする．$VU_0 = U$ つまり $V \equiv UU_0^\dagger$ を満たすように $V$ を定義する．これより $D(V,\ I) = \mathrm{tr}|V - I| = \mathrm{tr}|(U - U_0)U_0^\dagger| = \mathrm{tr}|U - U_0| < \epsilon(0)^2 < \epsilon(1)$．上で述べた補題 C.2 を繰り返し適用すると，$V$ の $\epsilon(1)^2$ 近似である $U_1 \in \mathcal{G}_{5l_0}$ が見出せる．したがって $U_1U_0$ は $U$ への $\epsilon(1)^2$ 近似である．いま $V'U_1U_0 = U$，つまり $V' \equiv UU_0^\dagger U_1^\dagger$ を満たすように $V'$ を定義する．これより $D(V',\ I) = \mathrm{tr}|V - I| = \mathrm{tr}|(U - U_1U_0)U_0^\dagger U_1^\dagger| = \mathrm{tr}|U - U_1U_0| < \epsilon(1)^2 < \epsilon(2)$ が成り立つ．補題 C.2 を反復適用すると $U_2 \in \mathcal{G}_{5^2 l_0}$ を見出すことができ，これ

は $V'$ への $\epsilon(2)^2$ 近似である．したがって $U_2U_1U_0$ は $U$ に対する $\epsilon(2)^2$ 近似である．この方法を続けると $U_k \in \mathcal{G}_{5^k l_0}$ を構築して，$U_kU_{k-1}\ldots U_0$ が $U$ への $\epsilon(k)^2$ 近似とすることができる．

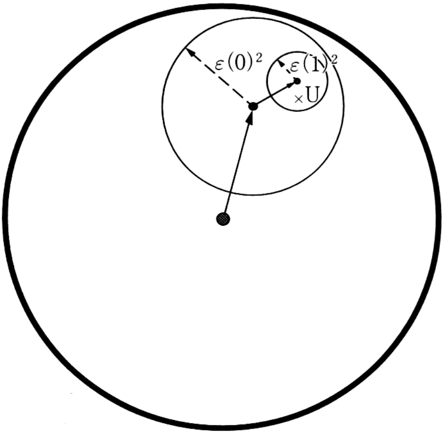



**図 C.1:** Solovay-Kitaev の定理の証明に用いる並進ステップ．任意の単一 q ビットゲート $U$ を近似するために，最初 $\mathcal{G}$ から $l_0$ 個のゲートを用いて距離 $\epsilon(0)^2$ 以内に近似する．次に $5l_0$ 個のゲートを追加してこの近似を改善して全精度を $\epsilon(1)^2$ よりも良くし，この方法を繰り返すと急速に $U$ に収束する．

すべてを総合すると一連の $l_0 + 5l_0 + \cdots + 5^k l_0 < \frac{5}{4}5^k l_0$ 個のゲートを用いて $\epsilon(k)^2$ の精度で任意のユニタリーゲート $U$ を近似できる．ある希望精度 $\epsilon$ で近似するには，次式を満たすように $k$ を選ばねばならない：

$$\epsilon(k)^2 < \epsilon. \tag{C.2}$$

式 (C.1) を代入するとこの式は

$$\left(\frac{3}{2}\right)^k < \frac{\log(1/C^2\epsilon)}{2\log(1/C\epsilon_0)}. \tag{C.3}$$

これから $\epsilon$ 以内で近似するに要するゲート数は，$c = \log 5/\log(3/2) \approx 4$ として

$$\text{ゲート数} < \frac{5}{4}5^k l_0 = \frac{5}{4}\left(\frac{3}{2}\right)^{kc} l_0 < \frac{5}{4}\left(\frac{\log(1/C^2\epsilon)}{2\log(1/C\epsilon_0)}\right)^c l_0. \tag{C.4}$$

つまり $\epsilon$ 以内で近似するのに必要なゲート数は $O(\log^c(1/\epsilon))$ となり，Solovay-Kitaev の定理が証明された．

補題 C.2 の証明には，次に再掲する $SU(2)$ 要素の積に関する二三の基本的事実を思い出そう．補題の中心となる考えは単位元の近傍を対象とすることであり，これにより $SU(2)$ の複雑な積演算が大いに簡単になる．正確に言えば $U$ と $V$ が $SU(2)$ の要素であるとして，$U$ と $V$ の**群交換子**(group commutator) を次式で定義する：

$$[U,\ V]_{\mathrm{gp}} \equiv UVU^\dagger V^\dagger. \tag{C.5}$$

$U$ と $V$ が両方とも単位元に近くて，$U = e^{-iA}$, $V = e^{-iB}$ と書けるとする．ここで $A$, $B$ はある小さな $\epsilon$ に対して $\mathrm{tr}|A|$, $\mathrm{tr}|B| \le \epsilon$ を満たす Hermite 行列である．$e^{\pm iA}$, $e^{\pm iB}$ を $A$, $B$ の 2 次まで展開すると

$$D([U,\ V]_{\mathrm{gp}},\ e^{-[A,\ B]}) = O(\epsilon^3), \tag{C.6}$$

ここで $[A,\ B] = AB - BA$ は通常の行列の交換子である（実際には $SU(2)$ の Lie 代数に対する交換子である）．したがって単位元近傍では群交換子を調べる代わりに，より簡単な行列交換子を調べればよい．

実際に q ビットに対して行列交換子は特に好ましい形をしている．$SU(2)$ の任意の要素はある実数ベクトル $\vec{a}$ に対して $U = u(\vec{a}) \equiv \exp(-i\vec{a}\cdot\vec{\sigma}/2)$ と書ける．同様にある実数ベクトル $\vec{b}$ に対して $V = u(\vec{b}) = \exp(-i\vec{b}\cdot\vec{\sigma}/2)$．演習 2.40 から

$$[\vec{a}\cdot\vec{\sigma},\ \vec{b}\cdot\vec{\sigma}] = 2i\left(\vec{a}\times\vec{b}\right)\cdot\vec{\sigma} \tag{C.7}$$

を思い出して，(C.6) より

$$D\big([U,\ V]_{\mathrm{gp}},\ u\big(\vec{a}\times\vec{b}\big)\big) = O(\epsilon^3). \tag{C.8}$$

これで補題 C.2 の証明における基本的考え方は容易に理解できる．詳細の大部分は近似法に関連しており完全な証明は後で記すが，さし当たり図 C.2 に示すようにまず主な概念を説明する．$S_{\epsilon^2}$ 中のある要素 $U = u(\vec{x})$ を近似するとする．演習 C.4 で見るように $D(U,\ I)$ のようなトレース距離は（ある補正を除いて）Euclid 距離 $\|\vec{x}\|$ に等しく，いい近似で $\|\vec{x}\| \le \epsilon^2$ である．$\vec{y}$ と $\vec{z}$ の長さを常にたかだか $\epsilon$ に選んで，$\vec{x} = \vec{y}\times\vec{z}$ を満たすことができる．$u(\vec{y}_0)$, $u(\vec{z}_0)$ が，$u(\vec{y})$, $u(\vec{z})$ をそれ

ぞれ $\epsilon^2$ 近似する $\mathcal{G}_l$ の要素となるように，$\vec{y_0}$，$\vec{z_0}$ を取り上げる．式 (C.6) を交換子 $[u(\vec{y}_0),\ u(\vec{z}_0)]_{\rm gp}$ に適用すると，$U$ に対する $O(\epsilon^3)$ 近似が得られる．これが $S_{\epsilon^2}$ に対する $O(\epsilon^3)$ ネットを与える．補題の証明を終えるには，Solovay-Kitaev の定理証明の主要部分で用いた並進ステップを適用すると，$5l$ 個のゲートで $S_{O(\epsilon^{3/2})}$ の任意の要素への $O(\epsilon^3)$ 近似が得られる．

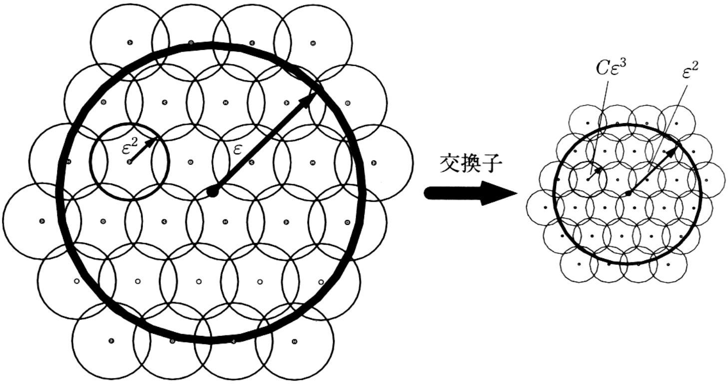



**図 C.2:** 補題 C.2 の証明の主要概念．$S_\epsilon$ 中の要素 $U_1$，$U_2$ の群交換子をとると $S_{\epsilon^2}$ をより稠密に満たす．右側に見える円の密度は左の円の各対当たり 1 つなければならないので，示しているよりももっと高密度であることに注意する．密度が低いのは単に見易くするためである．$S_{\sqrt{3}\epsilon^{3/2}}$ の任意の要素の良い近似を得るために，並進ステップ（図には示されていない）を適用すると，補題の証明が完成する．

**演習 C.2:** $A$，$B$ は Hermite 行列であり，$\mathrm{tr}|A|$, $\mathrm{tr}|B| \le \epsilon$ とする．十分小さなすべての $\epsilon$ とある定数 $d$ に対して

$$D\left([e^{-iA},\ e^{-iB}]_{\rm gp},\ e^{-[A,\ B]}\right) \le d\epsilon^3 \tag{C.9}$$

を証明せよ．これから式（C.6）が導ける．（コメント：実際に使用するには $d$ に対する良い限界が得られると興味深い．）

**演習 C.3:** $\vec{x}$, $\vec{y}$ は任意の実数ベクトルとする．次式を示せ．

$$D(u(\vec{x}),\ u(\vec{y})) = 2\sqrt{2}\sqrt{1-\cos\frac{x}{2}\cos\frac{y}{2}-\sin\frac{x}{2}\sin\frac{y}{2}\ \hat{x}\cdot\hat{y}}, \tag{C.10}$$

ここで $x \equiv \|\vec{x}\|$, $y \equiv \|\vec{y}\|$, $\hat{x}$, $\hat{y}$ はそれぞれ $\vec{x}$, $\vec{y}$ 方向の単位ベクトルである．

**演習 C.4:**　$\vec{y}=0$ の場合に $D(u(\vec{x}),\ u(\vec{y}))$ の式は次式になることを示せ．

$$D(u(\vec{x}),\ I) = 4\sin\left|\frac{x}{4}\right|. \tag{C.11}$$

**演習 C.5:**　$x,\ y \le \epsilon$ のとき次式を示せ．

$$D(u(\vec{x}),\ u(\vec{y})) = \|\vec{x}-\vec{y}\| + O(\epsilon^3). \tag{C.12}$$

**証明：(補題 C.2)**　$\mathcal{G}_l$ は $S_\epsilon$ における $\epsilon^2$ ネットであるとする．証明の第 1 ステップでは $[\mathcal{G}_l,\ \mathcal{G}_l]_{\rm gp}$ が $S_{\epsilon^2}$ とある定数 $C$ に対して $C\epsilon^3$ ネットであることを示す．

$U \in S_{\epsilon^2}$ として，$U = u(\vec{x})$ なる $\vec{x}$ を取り上げる．演習 C.4 より $x \le \epsilon^2 + O(\epsilon^6)$ が導ける．長さがたかだか $\epsilon + O(\epsilon^5)$ で $\vec{x} = \vec{y}\times\vec{z}$ を満たす任意のベクトル対 $\vec{y}$, $\vec{z}$ を選ぶ．$\mathcal{G}_l$ は $S_\epsilon$ に対する $\epsilon^2$ ネットなので

$$D(U_1, u(\vec{y})) < \epsilon^2 + O(\epsilon^5) \tag{C.13}$$

$$D(U_2, u(\vec{z})) < \epsilon^2 + O(\epsilon^5) \tag{C.14}$$

を満たすように，$\mathcal{G}_l \cap S_\epsilon$ 中で $U_1,\ U_2$ を選び，$U_1 = u(\vec{y}_0),\ U_2 = u(\vec{z}_0)$ を満たす $\vec{y}_0,\ \vec{z}_0$ を選ぶ．演習 C.4 より $y_0,\ z_0 \le \epsilon + O(\epsilon^3)$ が導ける．我々のゴールは $D(U,\ [U_1,\ U_2]_{\rm gp})$ は $C\epsilon^3$ より小さいことを示すことにある．このために三角不等式を用いる：

$$D(U,\ [U_1,\ U_2]_{\rm gp}) \le D\big(U, u(\vec{y}_0\times\vec{z}_0)\big) + D\big(u(\vec{y}_0\times\vec{z}_0),\ [U_1,\ U_2]_{\rm gp}\big). \tag{C.15}$$

演習 C.2 より第 2 項はたかだか $d'\epsilon^3$ である．ここで $d'$ は，$y_0,\ z_0 < \epsilon$ ではなく $y_0,\ z_0 < \epsilon + O(\epsilon^3)$ であるために生じ得る寄与により，$d$ より少し大きい定数である．$U = u(\vec{x})$ を代入し，演習 C.5 を用いて適切な定数 $d''$ を導入して簡単な代数計算を行うと

$$D(U,\ [U_1,\ U_2]_{\rm gp}) \le D\big(u(\vec{x}),\ u(\vec{y}_0\times\vec{z}_0)\big) + d'\epsilon^3 \tag{C.16}$$

$$= \|\vec{x} - \vec{y}_0\times\vec{z}_0\| + d''\epsilon^3 \tag{C.17}$$

$$= \|\vec{y}\times\vec{z} - \vec{y}_0\times\vec{z}_0\| + d''\epsilon^3. \tag{C.18}$$

$$= \|[(\vec{y} - \vec{y}_0) + \vec{y}_0] \times [(\vec{z} - \vec{z}_0) + \vec{z}_0] - \vec{y}_0 \times \vec{z}_0\| + d''\epsilon^3 \tag{C.19}$$

$$\leq (d'' + 2)\epsilon^3 + O(\epsilon^4) \tag{C.20}$$

$$\leq C\epsilon^3, \tag{C.21}$$

ここで $C$ は適切に選んだ定数である．

補題の証明の第 2 ステップでは，Solovay-Kitaev の定理証明の主要部分で用いたような，並進ステップを適用する．具体的に $U \in S_{\sqrt{C\epsilon^3}}$ が与えられると，$D(U,\ V) \leq \epsilon^2$，したがって $UV^\dagger \in S_{\epsilon^2}$ を満たす $V$ を $\mathcal{G}_l$ 中に見出すことができる．そうすると $D([W_1,\ W_2]_{\rm gp},\ UV^\dagger) \leq C\epsilon^3$ を満たす $W_1$，$W_2$ が $\mathcal{G}_l$ 中に見つかり，したがって

$$D([W_1,\ W_2]_{\rm gp}V,\ U) \leq C\epsilon^3 \tag{C.22}$$

よって証明された．□

**演習 C.6:** 基本ゲートの集合 $\mathcal{G}$ を固定して，次のアルゴリズムを記述せよ：単一 q ビットのユニタリーゲート $U$ の記述と希望精度 $\epsilon > 0$ が与えられたとき，$U$ を $\epsilon$ 近似する $\mathcal{G}$ の一連のゲートを効率良く計算せよ．

この付録の解析は少しおおまかなものであり，より厳密な解析が可能である．特に興味がある 1 つの問題は，限界 $O(\log^c(1/\epsilon))$ におけるベキ指数 $c$ の可能な最良値である．$c$ が 1 より小さくないことを示すのは難しくない．これを見るには $SU(2)$ において同じ半径 $\epsilon$ を有する $N$ 個の小さいボールの集まりを想像する．これらボールの体積はある重要でない定数 $d$ に対して $\epsilon^d$ のオーダである．したがって，もしボールで $SU(2)$ をカバーするとすれば $N$ は $\Omega(1/\epsilon^d)$ のオーダでなければならない．$\mathcal{G}$ から選んだ $g$ 個のゲートより成るすべての可能な列 $U_1U_2\ldots U_g$ を考える．明らかにこのような列はたかだか $|\mathcal{G}|^g$ 個の異なるユニタリー演算を作ることができる．したがって $|\mathcal{G}|^g = \Omega(1/\epsilon^d)$ でなければならず，これが求めるべきゲート数の下界を与える．

$$g = \Omega\left(\log\left(\frac{1}{\epsilon}\right)\right). \tag{C.23}$$

**問題 C.1:** この問題では任意の $c > 2$ に対して希望するターゲットを $\epsilon$ 以下で近似するに必要なゲート数に対して，上界 $O(\log^2(1/\epsilon)\log^c(\log(1/\epsilon)))$ を達成するためのより精密な証明のアウトラインを示す．

(1) $\mathcal{N}$ は $S_\epsilon$ における $\delta$ ネットであるとする．ここで $\epsilon_0$ は十分小さく，$0 < \delta < \epsilon \leq \epsilon_0$ である．ある定数 $d$ に対して，$[\mathcal{N}, \mathcal{N}]_{\rm gp}$ は $S_{\epsilon^2}$ における $d\delta\epsilon$ ネットであることを示せ．

(2) $0 < \delta < \epsilon \leq \epsilon_0$ に対して，$\mathcal{G}_l$ は $S_\epsilon$ における $\delta$ ネットであるとする．$\mathcal{G}_{4^k l}$ が $S_{\epsilon^{2^k}}$ における $d^k\delta\epsilon^{2^k-1}$ ネットであることを示せ．

(3) $k$ を

$$k \equiv \left\lceil \log\left(\frac{\log(1/\epsilon)}{\log(1/\epsilon_0)}\right)\right\rceil \tag{C.24}$$

で定義し，$\mathcal{G}_l$ は $S_{\epsilon_0}$ における $\delta_0$ ネットであるような $l$ が見い出せるとする．ここで

$$d^k\delta_0 = \epsilon_0 \tag{C.25}$$

である．$\mathcal{G}_{4^k l}$ は $S_{\epsilon_0^{2^k}}$ に対する $\epsilon$ ネットであることを示せ．

(4) すでに証明した形の Solvay-Kitaev の定理証明を用いて，$l = O(k^c)$ と選べばこの問題の前の部分には十分であることを示せ．ここで $c = \log(5)/\log(3/2)$ は Solvay-Kitaev の定理ですでに説明されたベキ指数に出てくる定数である．

(5) 前の結果を組み合わせて，$O(\log^2(1/\epsilon)\log^c(\log(1/\epsilon)))$ 個のゲートを用いると，$SU(2)$ の任意のゲートを $\epsilon$ 近似できることを証明せよ．

(6) 前の結果の結論において任意の $c > 2$ が可能であることを示せ．

**問題 C.2:** （研究）　前の問題で見出された結果よりも漸近的に速い近似手続きがもしあれば，それを見出せ．(a) 近似を行うに必要なゲート数が下界 $\Omega(\log(1/\epsilon))$ で飽和し，(b) そのようなゲートの近似手順を構築する効率的アルゴリズムが得られるのが理想である．

**問題 C.3:** （研究）　耐故障性を有し，単一 q ビットゲート — 例えば $\pi/8$ ゲートと Hadamard ゲート — で稠密な集合を生成する単一 q ビットゲートの有限集合 $\mathcal{G}$ を固定する．任意の単一 q ビットゲート $U$ と $\epsilon > 0$ が与えられたとき，グローバル位相を除いて $U$ の $\epsilon$ 近似を与える一連のゲートを耐故障性ゲート集合より作り出す簡潔，効率的かつ合理的にタイトな方法を開発せよ．

# 歴史と参考文献

この付録の結果は 1995 年に Solovay によって (未発表原稿), また独立に Kitaev によって証明された. Kitaev は証明の概略を [Kit97b] に示している. 同じ論文で Kitaev はこの結果を $SU(2)$ 以外に多くの Lie 群に一般化できることを見出した. 大まかに言えば証明に用いた $SU(2)$ に関する重要な事実は $[S_\epsilon, S_\epsilon]_{\mathrm{gp}} \supseteq S_{\Omega(\epsilon^2)}$ であり, この事実が成立する他の Lie 群も Solovay-Kitaev の定理のある版に従う. 例えば, 単位行列式を有する $d \times d$ ユニタリー行列の Lie 群 $SU(d)$ に対して Solovay-Kitaev の定理が成立する. この結果を聞いて Solovay はその後彼の証明を同じ様に一般化した. 我々の記述には Freedman による 1999 年の講義, および Freedmam, Kitaev, Solovay との討論から多くを得た.

# 付録D　整数論

暗号システムとそれを破るための量子コンピュータの使い方を理解するには基礎的整数論の理解が必要である．ここでは整数論に関する基本的事項を復習する．

## D.1　基　礎

最初に用語と記号について二三の慣用に従うこととする．**整数**の集合 $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$ を $\mathbf{Z}$ と表す．ときどき負でない整数を**自然数**と呼ぶことがあるが，ゼロを含むかどうかを区別するために**負でない整数** (非負整数，non-negative integer) か**正の整数** (positive integer) と呼ぶことが多い．

$n$ は整数であるとする．もし $n = dk$ なる整数 $k$ が存在するならば整数 $d$ は $n$ を**整除する**(divide) という（$d|n$ と書く）．この場合 $d$ は $n$ の**因数** (因子，factor) または**約数** (divisor) であるという．1 と $n$ は常に $n$ の因数である．$d$ が $n$ を整除しない（$d$ が $n$ の因数でない）ならば，$d \nmid n$ と書く．例えば $3|6$, $3|18$，しかし $3 \nmid 5$, $3 \nmid 7$ である．

**演習 D.1:（推移性）**　もし $a|b$ および $b|c$ ならば $a|c$ であることを示せ．

**演習 D.2:**　もし $d|a$, $d|b$ ならば $d$ は $a$ と $b$ の線形結合 $ax + by$ を整除することを示せ．ここで $x$, $y$ は整数である．

**演習 D.3:**　$a$, $b$ は正の整数であるとする．もし $a|b$ ならば $a \leq b$ であることを示せ．もし $a|b$ かつ $b|a$ ならば $a = b$ であることを示せ．

**素数** (prime number) はそれ自身と 1 だけを因数に持つ，1 より大きい整数である．最初の素数を幾つかあげると 2, 3, 5, 7, 11, 13, 17, ... である．多分正の整

数に関する最も重要な事実は，それらが素数である因数の積で一意に表現できることである．この結果には**数論の基本定理** (fundamental theorem of arithmetic) という印象的な名前が付けられている．

**定理 D.1:** **（数論の基本定理）** $a$ は 1 より大きい整数であるとする．このとき $a$ は次の形の**素因数分解** (prime factorization) を有する．

$$a = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}, \tag{D.1}$$

ただし $p_1, \dots, p_n$ は異なる素数，$a_1, \dots a_n$ は正の整数である．さらにこの素因数分解は因数の順序を除いて一意である．

**証明**　数論の基礎定理の証明を見たことのない読者には，自分自身で探してみることを強く勧める．もし見つからなければ基礎的な整数論の教科書に載っているので，付録 D の最後にある「歴史と参考資料」欄で教科書を見て欲しい．　□

小さい数に対して素因数分解を試行錯誤で見出すのは容易である．例えば $20 = 2^2 \cdot 5^1$ である．大きな数に対して古典コンピュータで素因数分解を見出す効率的アルゴリズムは，膨大な努力にもかかわらず知られていない．

**演習 D.4:** 697 と 36,300 の素因数分解を見出せ．

## D.2　剰余算と Euclid のアルゴリズム

我々は通常の整数論に精通しているとする．別の形の整数論，つまり**剰余算** (modular arithmmetic) は数の性質を知るうえで非常に有用である．読者が剰余整数論の基本概念に精通していると仮定して，上級の理論に進む前に基礎的考え方と記号について手早く見渡しておく．

剰余算は**剰余** (remainder) に関する計算である．18 を 7 で割れば答は 2 で剰余は 4 である．形式的には任意の正の整数 $x$ と $n$ が与えられると，$x$ は（一意に）次の形に書ける：

$$x = kn + r, \tag{D.2}$$

ここで負でない整数 $k$ は $x$ を $n$ で割った結果であり，**剰余** $r$ は 0 から $n-1$ の間の数である．剰余算は単に剰余にのみ注意を払う通常の計算である．剰余算で考

えていることを示すために記号 (mod $n$) を用いる．例えば 2, 5, 8, 11 は 3 で割るとすべて同じ剰余 2 になるので，$2=5=8=11 \pmod 3$ と書く．「(mod $n$)」なる名称は数 $n$ に関する剰余算表記である旨の注意を喚起している．

剰余算に対する加法，乗法および減法の定義は明らかであるが，おそらく除法の定義はそれほど自明ではない．この定義の仕方を理解するには，整数論のもう 1 つの重要な概念である 2 つの整数の**最大公約数** (gcd; greatest common divisor) を導入する．整数 $a$, $b$ の最大公約数は $a$ と $b$ の両方の約数のうちで最大の整数をいう．この数を gcd($a$, $b$) と書く．例えば 18 と 12 の最大公約数は 6 である．これを見る容易な方法は 18 (1, 2, 3, 6, 9, 18) と 12 (1, 2, 3, 4, 6, 12) の正の約数を計算し，2 つのリストから最大の共通な要素を取り上げる．この方法は大きな数に対して非常に非効率で実際的でない．幸い Euclid のアルゴリズムと呼ばれる最大公約数を効率的に計算する方法があり，以下数頁でこの説明を行う．

**定理 D.2:（gcd の表現定理）**　整数 $a$, $b$ の最大公約数は $ax+by$ の形で書ける最小の正の整数である．ここで $x$, $y$ は整数である．

**証明**　$s=ax+by$ をこの形に書ける最小の正の整数とする．gcd($a$, $b$) は $a$ と $b$ の約数なので $s$ の約数でもある．この結果 $\gcd(a,\ b)\le s$ である．証明を完成するために $s$ が $a$ と $b$ の約数であることを示して，$s\le\gcd(a,\ b)$ を示す．背理法で証明する．$s$ が $a$ の約数でないとする．このとき $a=ks+r$，ただし剰余 $r$ は 1 と $s-1$ の間の数である．式を整理し $s=ax+by$ を用いると，$r=a(1-kx)+b(-ky)$ は $a$ と $b$ の線形結合で書ける正の整数であり，$r$ は $s$ より小さい．しかしこれは $a$ と $b$ の線形結合で書ける最小の正の整数であるという $s$ の定義と矛盾する．したがって，$s$ は $a$ を整除すると結論される．対称性から $s$ は $b$ の約数でもあり，これで証明された．□

**系 D.3:**　$c$ は $a$ と $b$ の両方を整除するとする．このとき $c$ は gcd($a$, $b$) を整除する．

**証明**　定理 D.2 よりある整数 $x$, $y$ に対して $\gcd(a,\ b)=ax+by$ である．$c$ は $a$ と $b$ を整除するので $ax+by$ も整除する．□

数 $a$ が剰余算で乗算の逆数 (multiplicative inverse) の持つのはどのようなときか？ つまり $a$ と $n$ が与えられると，$ab = 1 \pmod n$ なる $b$ が存在するには如何なるときか？ 例えば $2 \cdot 3 = 1 \pmod 5$，したがって数 2 は 5 を法とする乗算の逆数 3 を持つ．他方で試行錯誤により 2 は 4 を法とする乗算の逆数を持たない．剰余算で乗算の逆数を見出すことは，**互いに素**(co-primality) の概念で gcd と関係していることがわかる：整数 $a$ $b$ は最大公約数が 1 であるならば互いに素であるという．例えば 14 と 9 は互いに素である．なぜなら 14 の正の約数は 1, 2, 7, 14，一方 9 の正の約数は 1, 3, 9 である．次の系は互いに素の性質を使って剰余算における乗算の逆数の存在を記述する．

**系 D.4:** $n$ は 1 より大きい整数であるとする．もし $\gcd(a,\ n) = 1$ つまり $a$ と $n$ が互いに素ならば，そのときにのみ整数 $a$ は $n$ を法とする乗法の乗算の逆数を持つ．

**証明**　$a$ は $n$ を法とする乗算の逆数を持つものとして，それを $a^{-1}$ と表す．このときある整数 $k$ に対して $aa^{-1} = 1 + kn$，したがって $aa^{-1} + (-k)n = 1$．定理 D.2 より $\gcd(a,\ n) = 1$ である．逆にもし $\gcd(a,\ n) = 1$ ならば $aa^{-1} + bn = 1$ なる整数 $a^{-1}$, $b$ が存在しなければならない．したがって $aa^{-1} = 1 \pmod n$ である．　□

**演習 D.5:** 素数 $p$ に対して 1 から $p-1$ の範囲のすべての整数が $p$ を法とする乗算の逆数を持つことを証明せよ．1 から $p^2-1$ の範囲のどのような数が $p^2$ を法とする乗算の逆数を持たないか？

**演習 D.6:** 24 を法とする 17 の乗算の逆数を求めよ．

**演習 D.7:** $n$ を 1 より大きな任意の整数として，$n^2$ を法とする $n+1$ の乗算の逆数を求めよ．

**演習 D.8:（逆数の一意性）**　$b,\ b'$ は $n$ を法とする $a$ の乗算の逆数であるとする．$b = b' \pmod n$ を証明せよ．

次の定理は正の 2 整数の最大公約数を求める Euclid の効率的アルゴリズムにとって鍵となるものである．

**定理 D.5:** $a$, $b$ は整数，$r$ は $a$ を $b$ で割ったときの剰余であるとする．$r \neq 0$ ならば

$$\gcd(a,\ b) = \gcd(b,\ r) \tag{D.3}$$

**証明** この等式の各辺が互いに他を整除するのを示して証明する．左辺が右辺を整除するのを示すにはある整数 $k$ に対して $r = a - kb$ であることを用いる．$\gcd(a,\ b)$ は $a$, $b$ とその線形結合を整除するので，$\gcd(a,\ b)$ は $r$ を整除する．系 D.3 より $\gcd(a,\ b)$ は $\gcd(b,\ r)$ を整除する．右辺が左辺を整除するのを示すには $\gcd(b,\ r)$ が $b$ を整除することを用いる．$a = r + kb$ は $b$ と $r$ の線形結合なので $\gcd(b,\ r)$ も $a$ を整除する．系 D.3 により $\gcd(b,\ r)$ は $\gcd(a,\ b)$ を整除する．□

**演習 D.9:** もし $a$ と $b$ の素因数分解がわかっているならば，$\gcd(a,\ b)$ を見出す方法を説明せよ．6825 と 1430 の素因数分解を見出し，それを使って $\gcd(6825,\ 1430)$ を計算せよ．

正の整数 $a$ と $b$ の最大公約数を見出す Euclid アルゴリズムは次のような働きをする．

(1) 最初に $a$, $b$ を $a > b$ の順に並べる．

(2) $a$ を $b$ で割り結果を $k_1$，剰余を $r_1$ とする：$a = k_1 b + r_1$
定理 D.5 より $\gcd(a,\ b) = \gcd(b,\ r_1)$

(3) $a$ の代わりに $b$, $b$ の代わりに $r_1$ として 2 回目の割り算をする：$b = k_2 r_1 + r_2$
定理 D.5 より $\gcd(a,\ b) = \gcd(b, r_1) = \gcd(r_1,\ r_2)$

(4) 次に $a$ の代わりに $r_1$，$b$ の代わりに $r_2$ として 3 回目の割り算をする：$r_1 = k_3 r_2 + r_3$
定理 D.5 より $\gcd(a,\ b) = \gcd(b, r_1) = \gcd(r_1,\ r_2) = \gcd(r_2,\ r_3)$

(5) この要領を続けて直近の剰余をその前の剰余で割り，新しい結果と剰余を得る．

(6) 剰余が 0 になるとアルゴリズムを停止する．つまりある $m$ に対して $r_m = k_{m+1} r_{m+1}$ $\gcd(a,\ b) = \gcd(r_m,\ r_{m+1}) = r_{m+1}$，したがってアルゴリズムは $r_{m+1}$ を返す．

Euclid のアルゴリズムの使い方の例として gcd(6825, 1430) を求める：

$$6825 = 4 \times 1430 + 1105 \tag{D.4}$$

$$1430 = 1 \times 1105 + 325 \tag{D.5}$$

$$1105 = 3 \times 325 + 130 \tag{D.6}$$

$$325 = 2 \times 130 + 65 \tag{D.7}$$

$$130 = 2 \times 65. \tag{D.8}$$

これから $\gcd(6825,\ 1430) = 65$ が求まる．

Euclid のアルゴリズムを改造して，$ax + by = \gcd(a,\ b)$ を満たす整数 $x$, $y$ を効率良く見つけるのに使用する．最初の段階は前と同じに Euclid のステップに従う．次の段階で Euclid アルゴリズムの下から 2 行目から出発して，以下の例に示すようにアルゴリズムの上の行を次々に代入していく：

$$65 = 325 - 2 \times 130 \tag{D.9}$$

$$= 325 - 2 \times (1105 - 3 \times 324) = -2 \times 1105 + 7 \times 325 \tag{D.10}$$

$$= -2 \times 1105 + 7 \times (1430 - 1 \times 1105) = 7 \times 1430 - 9 \times 1105 \tag{D.11}$$

$$= 7 \times 1430 - 9 \times (6825 - 4 \times 1430) = -9 \times 6825 + 43 \times 1430. \tag{D.12}$$

つまり $65 = 6825 \times (-9) + 1430 \times 43$ であり，これが希望した表現である．

Euclid のアルゴリズムで使われるリソースはどれくらいか？ $a$ と $b$ はたかだか各 $L$ ビット長のビット列で表されるとする．明らかに約数 $k_i$ と剰余 $r_i$ はいずれも $L$ ビット長以上ではなく，すべての計算が $L$ ビットの計算で行えると仮定できる．リソース解析の鍵は $r_{i+2} \le r_i/2$ に着目することである．これを証明するには 2 つの場合を考える：

- $r_{i+1} \le r_i/2$.　明らかに $r_{r+2} \le r_{i+1}$ であるので証明された．
- $r_{i+1} > r_i/2$.　この場合 $r_i = 1 \times r_{i+1} + r_{i+2}$ なので，
  $r_{i+2} = r_i - r_{i+1} \le r_i/2$ .

$r_{i+2} \le r_i/2$ なので，Euclid アルゴリズムの核心である「除算と剰余」の演算を行う回数は，たかだか $2\lceil \log a \rceil = O(L)$ 回である．各「除算と剰余」演算には $O(L^2)$ 回の演算を行うので，Euclid アルゴリズムの全コストは $O(L^3)$ である．

$ax + by = \gcd(a,\ b)$ なる $a,\ b$ を見出す付加的コストとしては僅か $O(L)$ 回の代入しか要しないので，全リソースコストは $O(L^3)$ である．

Euclid アルゴリズムは剰余算の乗算の逆数を効率良く求めるのにも使える．これは系 D.4 の証明に暗に含まれており，それを明示的に示す．$a$ は $n$ と互いに素であるとして，$n$ を法とする $a^{-1}$ を求めるとする．これを行うのに Euclid アルゴリズムと $a$ と $n$ が互いに素であることを使って

$$ax + ny = 1 \tag{D.13}$$

なる整数 $x,\ y$ を見出す．$ax = (1 - ny) = 1 \pmod n$，つまり $x$ は $n$ を法とする $a$ の乗算の逆数であることに留意する．さらにこのアルゴリズムの計算は効率的であり，$n$ のビット長を $L$ とすると $O(L^3)$ ステップしか要しない．

剰余算の逆数を効率良く見つける方法がわかったので，もう少しで次のような簡単な線形方程式が解ける：

$$ax + b = c \pmod n. \tag{D.14}$$

$a$ と $n$ は互いに素であるとする．Euclid アルゴリズムを用いて $n$ を法とする $a$ の乗算の逆数 $a^{-1}$ を効率良く求められ，上の方程式の解は

$$x = a^{-1}(c - b) \pmod n. \tag{D.15}$$

**中国剰余定理**[1](Chinese remainder theorem) と呼ぶ重要な結果により解ける方程式の範囲を広げることができて，剰余算の連立方程式を解くことができる．

**定理 D.6:** **(中国剰余定理)** $m_1, \ldots, m_n$ は正の整数で, 任意の対 $m_j,\ m_j,\ (i \neq j)$ は互いに素であるとする．このとき連立方程式

$$x = a_1 \pmod{m_1} \tag{D.16}$$

$$x = a_2 \pmod{m_2} \tag{D.17}$$

$$\cdots\cdots\cdots$$

$$x = a_n \pmod{m_n} \tag{D.18}$$

[1]訳注： 紀元 3 世紀頃中国の数学書「孫子算経」に「物不知数」問題として記されており，18 世紀になってヨーロッパに紹介された．

は解を持つ．さらに，この連立方程式の任意の 2 つの解は $M \equiv m_1 m_2 \ldots m_n$ を法として等しい．

**証明**　証明には連立方程式の解を明示的に求める．$M_i \equiv M/m_i$ を定義し，$m_i$ と $M_i$ が互いに素であることをみる．その結果 $M_i$ は $m_i$ を法とする逆数を持ち，それを $N_i$ と表す．$x \equiv \sum_i a_i M_i N_i$ を定義する．$x$ が連立方程式の解であることを見るには，$M_i N_i = 1 \pmod{m_i}$ および $i \neq j$ ならば $M_i N_i = 0 \pmod{m_j}$，したがって $x = a_i \pmod{m_i}$ に留意すると，$x = a_i \pmod{m_i}$ である．これで解の存在が示された．

$x$ と $x'$ の両方が連立方程式の解であるとする．各々の $i$ に対して $x - x' = 0 \pmod{m_i}$，したがって各 $i$ に対して $m_i$ は $x - x'$ を整除する．$m_i$ は互いに素なので積 $M = m_1 \ldots m_n$ も $x - x'$ を整除し，したがって $x = x' \pmod{M}$ である．よって証明された．□

Euclid アルゴリズムと中国剰余定理は注目すべき整数論アルゴリズムの勝利である．整数論のあるアルゴリズムを実行する**困難さ**に安全性の基礎を置いている RSA 暗号システムを導く一連の概念において，これらが重要な役割を果たしているといってもまんざら皮肉ではない．これは事実なのである！ 次に RSA 暗号システムを理解するのに必要な整数論的背景に話を変える．鍵となる概念は古典的整数論の有名な結果である **Fermat の小定理** (Fermat's little theorem) —Fermat の最終定理と混同してはならない—と Euler による Fermat の小定理の一般化である．

**補題 D.7:**　$p$ は素数，$k$ は 1 から $p-1$ の範囲の整数である．このとき $p$ は $\binom{p}{k}$ を整除する．

**証明**　恒等式

$$p(p-1)\cdots(p-k+1) = \binom{p}{k} k(k-1)\cdots 1 \tag{D.19}$$

を考える．$k \geq 1$ なので右辺は（したがって左辺も）$p$ で割れる．$k \leq p-1$ なので項 $k(k-1)\cdots 1$ は $p$ で割れない．したがって $\binom{p}{k}$ は $p$ で整除される．□

**定理 D.8:**　**（Fermat の小定理）**　$p$ は素数，$a$ は任意の整数とする．このとき $a^p = a \pmod{p}$ である．もし $a$ が $p$ で割り切れなければ $a^{p-1} = 1 \pmod{p}$ である．

**証明**　もし $a$ が $p$ で整除できなければ $a$ は $p$ を法とする逆数を有し，$a^{p-1} = a^{-1}a^p = a^{-1}a = 1 \pmod p$ であるので，定理の第 2 部分は第 1 部分から導ける．正の $a$ に対して定理の最初の部分を $a$ に関する帰納法で証明する（正でない $a$ の場合は容易に証明できる）．$a = 1$ のときは要求通り $a^p = 1 = a \pmod p$ である．$a$ に対して定理の結果つまり $a^p = a \pmod p$ が成立するとして $a+1$ の場合を考える．2 項展開により

$$(1+a)^p = \sum_{k=0}^{p} \binom{p}{k} a^k. \tag{D.20}$$

補題 D.7 より $1 \le k \le p-1$ ならば $p$ は $\binom{p}{k}$ を整除するので，$p$ を法とする総和から最初と最後の項以外は消えて $(1+a)^p = (1+a^p) \pmod p$ となる．帰納法の仮定 $a^p = a \pmod p$ を適用すると，要求通り $(1+a)^p = (1+a) \pmod p$ が示せる．□

**Euler の $\varphi$ 関数** (Euler $\varphi$ function) を用いた Euler による有名な Fermat 小定理の一般化がある．$\varphi(n)$ は $n$ より小さく $n$ と互いに素な正の整数の数であると定義する．例えば素数 $p$ より小さなすべての正の整数は $p$ と互いに素であり，したがって $\varphi(p) = p-1$ である．$p^\alpha$ より小さく $p^\alpha$ と互いに素でない整数は $p$ の倍数，つまり $p,\ 2p,\ 3p,\ \ldots, (p^{\alpha-1}-1)p$ である．これから次式が推論される

$$\varphi(p^\alpha) = (p^\alpha - 1) - (p^{\alpha-1} - 1) = p^{\alpha-1}(p-1). \tag{D.21}$$

さらに，もし $a$ と $b$ が互いに素ならば中国剰余定理を用いて次式を示せる．

$$\varphi(ab) = \varphi(a)\varphi(b). \tag{D.22}$$

これを調べるには連立方程式 $x = x_a \pmod a$, $x = x_b \pmod b$ を考える．この連立方程式に中国剰余定理を適用すると，$1 \le x_a < a$, $1 \le x_b < b$, $\gcd(x_a,\ a) = 1$, $\gcd(x_b,\ b) = 1$ なる対 $(x_a,\ x_b)$ と，$1 \le x < ab$, $\gcd(x,\ ab) = 1$ なる整数 $x$ との間に 1 対 1 の対応が存在する．$\varphi(a)\varphi(b)$ 個のそのような対 $(x_a,\ x_b)$ と $\varphi(ab)$ 個のそのような $x$ が存在し，これから式 (D.22) が推論される．

式 (D.21) と式 (D.22) は $n$ の素因数分解 $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ に基づく $\varphi(n)$ に対する次式を意味している：

$$\varphi(n) = \prod_{j=1}^{k} p_j^{\alpha_j - 1}(p_j - 1). \tag{D.23}$$

**演習 D.10:** $\varphi(187)$ は何か？

**演習 D.11:** 次式を証明せよ：

$$n = \sum_{d|n} \varphi(d), \tag{D.24}$$

ここで総和は 1 と $n$ を含む $n$ のすべての正の約数 $d$ について行う．（ヒント：最初に $n = p^\alpha$ に対して証明し，次に式 (D.22) で示した $\varphi$ の積の性質を使うと証明できる．）

Fermat の小定理は Euler による次のような簡潔な一般化ができる．

**定理 D.9:** $a$ は $n$ と互いに素であるとする．このとき $a^{\varphi(n)} = 1 \pmod{n}$ である．

**証明**　最初に $\alpha$ に関する帰納法で $a^{\varphi(p^\alpha)} = 1 \pmod{p^\alpha}$ を示す．$\alpha = 1$ に対しては，この結果は Fermat の小定理そのものである．$\alpha \geq 1$ に対して結果が成立すると仮定すると，ある整数 $k$ に対して

$$a^{\varphi(p^\alpha)} = 1 + kp^\alpha. \tag{D.25}$$

式 (D.21) より

$$\begin{aligned} a^{\varphi(p^{\alpha+1})} &= a^{p^\alpha(p-1)} && \text{(D.26)} \\ &= a^{p\varphi(p^\alpha)} && \text{(D.27)} \\ &= (1 + kp^\alpha)^p && \text{(D.28)} \\ &= 1 + \sum_{j=1}^{p} \binom{p}{j} k^j p^{j\alpha}. && \text{(D.29)} \end{aligned}$$

補題 D.7 を用いると $p^{\alpha+1}$ は総和のすべての項を整除するので

$$a^{\varphi(p^{\alpha+1})} = 1 \pmod{p^{\alpha+1}}, \tag{D.30}$$

これで帰納法により証明された．任意の $n = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$ に対して，$\varphi(n)$ は $\varphi(p_j^{\alpha_j})$ の倍数なので各々の $j$ に対して $a^{\varphi(n)} = 1 \pmod{p_j^{\alpha_j}}$ を用いると，定理の証明が完成する．中国剰余定理の証明で用いた構成を適用すると，連立方程式 $x = 1 \pmod{p_j^{\alpha_j}}$ の任意の解は $x = 1 \pmod n$，したがって $a^{\varphi(n)} = 1 \pmod n$ を満たさなければならない． □

$\mathbf{Z}_n^*$ は $n$ を法とする逆数を持つ $\mathbf{Z}_n$ のすべての要素の集合であると定義する．つまり $n$ と互いに素な $\mathbf{Z}_n$ 中のすべての要素の集合である．$\mathbf{Z}_n^*$ は乗算のもとでサイズ $\varphi(n)$ の群を形成するのが容易にわかる，つまり $\mathbf{Z}_n^*$ は乗算の単位元を含み，$\mathbf{Z}_n^*$ の要素の積は $\mathbf{Z}_n^*$ に存在し，$\mathbf{Z}_n^*$ は乗算の逆数演算のもとで閉じている（基礎的群論の概説は付録 B 参照）．$n$ が奇の素数のベキであるとき，つまり $n = p^\alpha$ のときに $\mathbf{Z}_n^*$ が持つ顕著な構造は自明ではない．$\mathbf{Z}_{p^\alpha}^*$ は**巡回群** (cyclic group) であることがわかっている．つまり $\mathbf{Z}_{p^\alpha}^*$ には要素 $g$ が存在し，ある負でない整数 $k$ に対して任意の他の要素 $x$ が $x = g^k \pmod n$ と書けるという意味で，$g$ は $\mathbf{Z}_{p^\alpha}^*$ を**生成** (generate) する．

**定理 D.10:** $p$ は奇の素数，$\alpha$ は正の整数とすると，$\mathbf{Z}_{p^\alpha}^*$ は巡回的である．

**証明** この事実の証明は本書の範囲を少し超えている．整数論を含む多くの教科書に見出すことができる．例えば Knuth [Knu98a] の 3.2 節，特に 16 頁から 23 頁を参照． □

**演習 D.12:** $\mathbf{Z}_n^*$ は $n$ を法とする乗算演算のもとで，サイズ $\varphi(n)$ の群を形成することを証明せよ．

**演習 D.13:** $a$ は $\mathbf{Z}_n^*$ の任意の要素である．$S \equiv \{1,\ a,\ a^2, \ldots\}$ は $\mathbf{Z}_n^*$ の部分群を形成すること，および $S$ のサイズは少なくとも $a^r = 1 \pmod n$ なる $r$ であることを示せ．

**演習 D.14:** $g$ は $\mathbf{Z}_n^*$ の生成元である．$g$ は位数 $\varphi(n)$ を持たねばならないことを示せ．

**演習 D.15:** 定理 B.1 の **Lagrange の定理** (Lagrange's theorem) は部分群のサイズが群の位数を整除することを記述する群論の基本的結果である．Lagrange の定理を用いて定理 D.9 の別の証明を示せ．つまり任意の $a \in \mathbf{Z}_n^*$ に対して $a^{\varphi(n)} = 1 \pmod{n}$ が成り立つことを示せ．

## D.3　素因数分解から位数発見への縮約

古典コンピュータ上で数の素因数分解を求める問題は他の問題，つまり**位数発見** (order-finding) 問題と等価であることがわかっている．量子コンピュータが位数発見問題を高速で解くことができ，したがって素因数分解が高速でできることがわかるので，この等価性は重要である．本節では素因数分解を位数発見に縮約することに焦点を絞って，この 2 つの問題の等価性を説明する．

$N$ は正の整数，$x$ は $N$ と互いに素（$1 \leq x < N$）であるとする．$N$ を法とする $x$ の**位数** (order) とは $x^r = 1 \pmod{N}$ なる最小の正の整数 $r$ であると定義する．**位数発見問題**は $x$ と $N$ が与えられたときに $r$ を決定することである．

**演習 D.16:** 定理 D.9 を用いて $N$ を法とする $x$ の位数は $\varphi(N)$ を整除することを示せ．

素因数分解を位数発見に縮約するには 2 つの基本的ステップで進める．最初のステップでは，方程式 $x^2 = 1 \pmod{N}$ に対する有意の解 $x \neq \pm 1 \pmod{N}$ を見出すことができるならば，$N$ の素因数が計算できることを示す．第 2 ステップでは，$N$ と互いの素でランダムに選んだ $y$ は $y^{r/2} \neq \pm 1 \pmod{N}$ なる偶の位数 $r$ を持ち，したがって $x \equiv y^{r/2} \pmod{N}$ が $x^2 = 1 \pmod{N}$ の解であることを示す．

**定理 D.11:** $N$ は $L$ ビット長の合成数，$x$ は方程式 $x^2 = 1 \pmod{N}$ に対する $1 \leq x \leq N$ の範囲の有意な解であるとする．つまり $x = 1 \pmod{N}$ でもなく，$x = N - 1 = -1 \pmod{N}$ でもない．このとき $\gcd(x-1,\ N)$ と $\gcd(x+1,\ N)$ の少なくとも一方が $N$ の有意の素因数であり $O(L^3)$ 回の演算で計算できる．

**証明**　$x^2 = 1 \pmod N$ なので $N$ は $x^2-1=(x+1)(x-1)$ を整除できなければならず，したがって $N$ は $(x+1)$ か $(x-1)$ のいずれかと公約数を持つ．しかし仮定より $1 < x < N-1$ なので $x-1 < x+1 < N$，これから公約数は $N$ 自身ではあり得ない．Euclid のアルゴリズムを用いて $\gcd(x-1,\ N)$ と $\gcd(x+1,\ N)$ を計算することができて，$O(L^3)$ 回の演算で有意の素因数 $N$ が得られる．　□

**補題 D.12:**　$p$ は奇の素数である．$2^d$ は $\varphi(p^\alpha)$ を整除する最大の 2 のベキ乗であるとする．このとき正確に確率 1/2 で $2^d$ は，ランダムに選んだ $\mathbf{Z}_{p^\alpha}^*$ の要素 $p^\alpha$ を法とする位数を整除する．

**証明**　$p$ は奇数なので $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$ は偶数であり，したがって $d \geq 1$ である．定理 D.10 より $\mathbf{Z}_{p^\alpha}^*$ に対する生成元 $g$ が存在し，1 から $\varphi(p^\alpha)$ の間のある $k$ に対して，任意の要素が $g^k \pmod{p^\alpha}$ の形で書ける．$r$ が $p^\alpha$ を法とする $g^k$ の位数であるとする．最初のケースは $k$ が奇数とする．$g^{kr} = 1 \pmod{p^\alpha}$ から $\varphi(p^\alpha)|kr$ が導かれ，$k$ が奇数なので $2^d|r$ である．第 2 のケースは $k$ が偶数とする．このとき

$$g^{k\varphi(p^\alpha)/2} = \left(g^{\varphi(p^\alpha)}\right)^{k/2} = 1^{k/2} = 1 \pmod{p^\alpha}. \tag{D.31}$$

したがって $r|\varphi(p^\alpha)/2$，これより $2^d$ は $r$ を整除しないことがわかる．

まとめると，$\mathbf{Z}_{p^\alpha}^*$ は等サイズの 2 つの集合に分けることができる．一方は奇数の $k$ を用いて $g^k$ と書けて，$g^k$ の位数 $r$ に対して $2^d|r$ である．他方は偶数の $k$ を用いて $g^k$ と書けて，$2^d \nmid r$ である．したがって，確率 1/2 で整数 $2^d$ は $\mathbf{Z}_{p^\alpha}^*$ からランダムに選んだ要素の位数 $r$ を整除し，確率 1/2 で整除しない．　□

**定理 D.13:**　$N = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$ は奇の合成数の素因数分解であるとする．$x$ を $\mathbf{Z}_N^*$ から一様かつランダムに選び，$r$ を $N$ を法とする $x$ の位数とすると

$$p\big(r\,\text{が偶，かつ}\ x^{r/2} \neq -1 \pmod N\big) \geq 1 - \frac{1}{2^{m-1}}. \tag{D.32}$$

**証明**　我々は

$$p\big(r\,\text{が奇，かつ}\ x^{r/2} \neq -1 \pmod N\big) \leq \frac{1}{2^{m-1}} \tag{D.33}$$

を示す．中国剰余定理より，$\mathbf{Z}_N^*$ から $x$ を一様かつランダムに選ぶことは，$\mathbf{Z}_{p_j^{\alpha_j}}$ から $x_j$ を独立に一様かつランダムに選び，各 $j$ に対して $x = x_j \pmod{p_j^{\alpha_j}}$ と

要求するのと等価である．$r_j$ は $p_j^{\alpha_j}$ を法とする $x_j$ の位数であるとする．$2^{d_j}$ は $r_j$ を整除する最大の 2 のベキ数であり，$2^d$ は $r$ を整除する最大の 2 のベキ数であるとする．$r$ が奇数，もしくは $x^{r/2} = -1 \pmod N$ であるためには，$d_j$ がすべての $j$ の値に対して同じ値をとらなければならないことを示そう．補題 D.12 より $d_2, \ldots, d_m$ は $d_1$ に等しく，各々が確率を 1/2 ずつ下げるので結果はたかだか $1/2^{m-1}$ となる．

最初に我々が考えるのは $r$ が奇数の場合である．各 $j$ に対して $r_j|r$ が容易に示せて $r_j$ が奇数となるので，すべての $i = 1, \ldots, k$ に対して $d_j = 0$ である．第 2 の $r$ が偶数で $x^{r/2} = -1 \pmod N$ の場合には $x^{r/2} = -1 \pmod{p_j^{\alpha_j}}$ したがって $r_j \nmid (r/2)$ である．$r_j|r$ なのですべての $j$ に対して $d_j = d$ でなければならない．

□

定理 D.11 と定理 D.13 を組み合わせると，任意の合成数 $N$ の有意の素因数を高い確率で返すアルゴリズムが得られる．このアルゴリズムの全ステップは古典コンピュータで効率良く行えるが，（現在わかっている）例外はこのアルゴリズムで用いられる位数発見「サブルーチン」である．アルゴリズムを繰り返すと $N$ の完全な素因数分解を見つけることができる．アルゴリズムを次にまとめる．

(1) $N$ が偶数ならば因数 2 を返す．

(2) 演習 5.17 のアルゴリズムを用いて整数 $a \geq 1$, $b \geq 1$ に対して $N = a^b$ かどうかを決めて，もしそうならば因数 $a$ を返す．

(3) 1 と $N-1$ の範囲で $x$ をランダムに選び，もし $\gcd(x, N) > 1$ ならば因数 $\gcd(x, N)$ を返す．

(4) 位数発見サブルーチンを用いて $N$ を法とする $x$ の位数 $r$ を見つける．

(5) もし $r$ が偶数で $x^{r/2} \neq -1 \pmod N$ ならば，$\gcd(x^{r/2}-1, N)$ と $\gcd(x^{r/2}+1, N)$ を計算し，有意な因数であることを調べてそれを返す．そうでなければアルゴリズムは成立しない．

アルゴリズムのステップ 1 と 2 は因数を返すか，そうでなければ $N$ は奇の整数で 1 つ以上の素因数を持つことが確認される．このステップはそれぞれ $O(1)$ と $O(L^3)$ 回の演算で実行できる．ステップ 3 は因数を返すか，あるいは $\mathbf{Z}_N^*$ のランダムに選んだ要素 $x$ を作る．ステップ 4 は位数発見サブルーチンを呼び出

し，$N$ を法とする $x$ の位数 $r$ を計算する．少なくとも確率 1/2 で $r$ は偶数で $x^{r/2} \neq -1 \pmod N$ であることが定理 D.13 で保証され，$\gcd(x^{r/2}-1,\ N)$ か $\gcd(x^{r/2}+1,\ N)$ のいずれかが $N$ の有意な因数となることが定理 D.11 で保証されるので，ステップ 5 でアルゴリズムが終了する．

**演習 D.17:（位数発見から素因数分解への縮約）** 効率的位数発見アルゴリズムによって素因数分解が効率良くできることがわかった．効率的な素因数分解アルゴリズムがあれば $N$ と互いに素な任意の $x$ の $N$ を法とする位数が効率的に見つけられることを示せ．

# D.4　連分数

連続な実数と整数の間には多くの顕著な関連性がある．そのような関係の 1 つが**連分数** (continued fraction) である．本節では連分数理論の二三の要素，つまり 5 章で述べる位数発見や素因数分解に対する高速量子アルゴリズムへの応用おいて重要な要素を学ぶ．

連分数の例として次式で与えられる数 $s$ を考える．

$$s \equiv \frac{1}{2+\frac{1}{2+\frac{1}{2+\cdots}}}. \tag{D.34}$$

非公式には $s = 1/(2+s)$ とおくと容易に $s = \sqrt{2}-1$ が導ける．連分数法の概念は式 (D.34) のような表現により実数を整数だけで記述することである．**有限単純連分数**は有限の正の整数の集まり $a_0,\ \ldots, a_N$

$$[a_0,\ldots,a_N] \equiv a_0 + \frac{1}{a_1+\frac{1}{a_2+\frac{1}{\cdots+\frac{1}{a_N}}}} \tag{D.35}$$

で定義される．この連分数に対する $n$ 番目の収束値（$0 \leq n \leq N$）を $[a_0,\ldots,a_n]$ と定義する．

**定理 D.14:** $x$ は 1 より大きいか等しい有理数とする．このとき $x$ は連分数の表現 $x = [a_0,\ldots,a_N]$ を有し，**連分数アルゴリズム**で求められる．

**証明**　連分数アルゴリズムを理解するには例を使うのが一番良い．31/13 を連分数に分解することを試みる．連分数アルゴリズムの第 1 ステップは 31/13 を整数部分と分数部分に分離する．

$$\frac{31}{13} = 2 + \frac{5}{13}. \tag{D.36}$$

次に分数部分を反転する：

$$\frac{31}{13} = 2 + \frac{1}{\frac{13}{5}}. \tag{D.37}$$

このステップ — 分離と反転 — を 13/5 に適用すると

$$\frac{31}{13} = 2 + \frac{1}{2 + \frac{3}{5}} = 2 + \frac{1}{2 + \frac{1}{\frac{5}{3}}}. \tag{D.38}$$

次に 5/3 を分離・反転すると：

$$\frac{31}{13} = 2 + \frac{1}{2 + \frac{1}{1+\frac{2}{3}}} = 2 + \frac{1}{2 + \frac{1}{1+\frac{1}{\frac{3}{2}}}}. \tag{D.39}$$

3/2=1+1/2 は反転しなくても分子が 1 と書けるので連分数への分解はここで終わり，31/13 の最終的な連分数表現は次のようになる．

$$\frac{31}{13} = 2 + \frac{1}{2 + \frac{1}{1+\frac{1}{1+\frac{1}{2}}}}. \tag{D.40}$$

現れる分子（上の例では 31, 3, 3, 1）は確実に減少するので，任意の有理数に対する連分数アルゴリズムは有限回の「分離と反転」ステップで終了する．どれくらい早く終了するか？ 間もなくこの疑問に答える．　□

上の定理は $x \geq 1$ に対して述べられている．しかし実際には $a_0$ が正という要求を緩めて任意の整数とするのが便利であり，その結果 $x \geq 1$ という制約は無用になる．特に量子アルゴリズムの応用にあるように，もし $x$ が 0 と 1 の範囲にあるならば連分数展開は $a_0 = 0$ となる．

連分数アルゴリズムは与えられた有理数の連分数展開を得る曖昧さのない方法である．唯一曖昧さが生じるとすればそれは最終段階であり，整数を分離するの

に 2 つの方法がある．つまり $a_n = a_n$ とするか $a_n = (a_n - 1) + 1/1$ とするかで 2 つの別の連分数展開となる．実際にはこの曖昧さによって，与えられた有理数が持つ収束値の数を奇とするか偶とするかを一般性を失うことなく望み通りに仮定できるので便利である．

**演習 D.18:** $x = 19/17$ と $x = 77/65$ に対する連分数展開を求めよ．

**定理 D.15:** $a_0, \ldots, a_N$ は正の数列である．このとき

$$[a_0, \ldots, a_n] = \frac{p_n}{q_n}, \tag{D.41}$$

ここで $p_n$，$q_n$ は実数であり，$p_0 \equiv a_0$，$q_0 \equiv 1$，$p_1 \equiv 1 + a_0 a_1$，$q_1 \equiv a_1$，$2 \le n \le N$ に対して

$$p_n \equiv a_n p_{n-1} + p_{n-2} \tag{D.42}$$

$$q_n \equiv a_n q_{n-1} + q_{n-2} \tag{D.43}$$

により帰納的に定義する．$a_j$ が正の整数の場合には $p_j$，$q_j$ も正の整数である．

**証明** $n$ に関する帰納法で証明する．$n = 0$, $1$, $2$ に対しては直接容易に検証できる．$n \ge 3$ に対して定義より

$$[a_0, \ldots,\ a_n] = [a_0, \ldots, a_{n-2},\ a_{n-1} + 1/a_n]. \tag{D.44}$$

帰納法の仮定を適用し，$\tilde{p}_j/\tilde{q}_j$ を右辺の連分数展開に関連した収束値数列であるとすると

$$[a_0, \ldots, a_{n-2},\ a_{n-1} + 1/a_n] = \frac{\tilde{p}_{n-1}}{\tilde{q}_{n-1}}. \tag{D.45}$$

明らかに $\tilde{p}_{n-3} = p_{n-3}$，$\tilde{p}_{n-2} = p_{n-2}$ および $\tilde{q}_{n-3} = q_{n-3}$，$\tilde{q}_{n-2} = q_{n-2}$ なので

$$\frac{\tilde{p}_{n-1}}{\tilde{q}_{n-1}} = \frac{(a_{n-1} + 1/a_n)p_{n-2} + p_{n-3}}{(a_{n-1} + 1/a_n)q_{n-2} + q_{n-3}} \tag{D.46}$$

$$= \frac{p_{n-1} + p_{n-2}/a_n}{q_{n-1} + q_{n-2}/a_n}. \tag{D.47}$$

右辺の分母分子に $a_n$ を掛けると

$$\frac{\tilde{p}_{n-1}}{\tilde{q}_{n-1}} = \frac{p_n}{q_n}. \tag{D.48}$$

式 (D.48), (D.45), (D.44) を組み合わせると

$$[a_0, \dots, a_n] = \frac{p_n}{q_n}. \tag{D.49}$$

これで証明された. □

**演習 D.19:** $n \geq 1$ に対して $q_n p_{n-1} - p_n q_{n-1} = (-1)^n$ を示せ. この事実を使って $\gcd(p_n, q_n) = 1$ を証明せよ. (ヒント: $n$ に関する帰納法を使え.)

$p$ と $q$ が互いに素であるとき, 有理数 $x = p/q > 1$ に対する連分数展開を得るには, 幾つの $a_n$ を決定しなければならないか? $a_0, \dots, a_N$ が正の整数であるとする. $p_n$, $q_n$ の定義より $p_n$ と $q_n$ は増大する数列であることがわかる. したがって $p_n = a_n p_{n-1} + p_{n-2} \geq 2p_{n-2}$, 同様に $q_n \geq 2q_{n-2}$, これから $p_n, q_n \geq 2^{\lfloor n/2 \rfloor}$ が導かれる. したがって $2^{\lfloor N/2 \rfloor} \leq q \leq p$, したがって $N = O(\log(p))$ である. この結果もし $x = p/q$ が有理数ならば $p$ と $q$ は $L$ ビットの整数であり, $x$ に対する連分数展開は $O(L^3)$ 回の演算で — $O(L)$ 回の「分離と反転」ステップと, それぞれの基本的計算に $O(L^2)$ 個のゲートを使用して — 計算できる.

**定理 D.16:** $x$ は有理数, $p/q$ は次式を満たす有理数とする:

$$\left| \frac{p}{q} - x \right| \leq \frac{1}{2q^2}. \tag{D.50}$$

このとき $p/q$ は $x$ に対する連分数の収束値である.

**証明**　$p/q = [a_0, \dots, a_n]$ を $p/q$ に対する連分数であるとして, $p_j$, $q_j$ を定理 D.15 のように定義する. その結果 $p_n/q_n = p/q$ である. $\delta$ を次式で定義する.

$$x \equiv \frac{p_n}{q_n} + \frac{\delta}{2q_n^2}, \tag{D.51}$$

したがって $|\delta| < 1$. 次のように $\lambda$ を定義する.

$$\lambda \equiv 2\left( \frac{q_n p_{n-1} - p_n q_{n-1}}{\delta} \right) - \frac{q_{n-1}}{q_n}. \tag{D.52}$$

このように $\lambda$ を定義する理由は少し計算すると次式を満たすことが示せて

$$x = \frac{\lambda p_n + p_{n-1}}{\lambda q_n + q_{n-1}}, \tag{D.53}$$

したがって $x = [a_0, \ldots, a_n,\ \lambda]$ となるからである．$n$ を偶数に選ぶと演習 D.19 より

$$\lambda = \frac{2}{\delta} - \frac{q_{n-1}}{q_n}. \tag{D.54}$$

$q_n$ が増大する性質を持つので

$$\lambda = \frac{2}{\delta} - \frac{q_{n-1}}{q_n} > 2 - 1 \geq 1. \tag{D.55}$$

したがって $\lambda$ は 1 より大きな有理数であり，単純有限連分数 $\lambda = [b_0, \ldots, b_m]$ を持ち，したがって $x = [a_0, \ldots, a_n, b_0, \ldots, b_m]$ は $p/q$ を収束値とする $x$ に対する単純有限連分数である． □

**問題 D.1:（素数推定）**　$\pi(n)$ を $n$ より小さい素数の数とする．**素数定理**と呼ぶ証明が難しい定理があり，その結果によれば $\lim_{n\to\infty} \pi(n)\log(n)/n = 1$，したがって $\pi(n) \approx n/\log(n)$ である．この問題は貧者の素数定理を与えるもので，素数分布に関するかなり良い下界を与える．

(1) 次式を証明せよ．

$$n \leq \log \binom{2n}{n}.$$

(2) 次式を示せ．ここで総和は $2n$ より小さいか等しいすべての素数 $p$ について行う．

$$\log \binom{2n}{n} \leq \sum_{p \leq 2n} \left\lfloor \frac{\log(2n)}{\log p} \right\rfloor \log p. \tag{D.56}$$

(3) 前の 2 つの結果を用いて次式を示せ．

$$\pi(2n) \geq \frac{n}{\log(2n)}. \tag{D.57}$$

## 歴史と参考資料

整数論には優れた教科書が多い．我々がかなり利用した Koblitz [Kob94] は整数論，アルゴリズム，および暗号をひとまとめにして関連づけている．同様の組み合わせをアルゴリズム向けに一般化した記述が Cormen, Leiserson, Rivest [CLR90] の第 33 章で見られる．連分数に関する我々の議論は整数論の古典的教科書 Hardy, Wright [HW60] の第 10 章に基づいている．問題 D.1 は Papadimitriou [Pap94] によっている．

# 付録E　公開鍵暗号とRSA暗号システム

暗号は2人の当事者が私的に通信をする技術である．例えば，消費者がインターネット上で買い物をしたい会社だけにわかるように，クレジットカード番号をインターネットで知らせたいとする．もっと険悪な事態では，戦時に交戦中の国が秘密の通信をする手段を必要とすることもある．プライバシーを確保するために**暗号プロトコル** (cryptographic prtocol) あるいは**暗号システム** (cryptosystem) が用いられる．実効的な暗号システムは互いに通信する当事者には使い易く，第三者が会話の内容を「盗聴」するのが困難なものでなければならない．

特に重要な暗号システムは**公開鍵暗号** (public key cryptosystem) である．公開鍵暗号の基本的アイディアは図 E.1 にアナロジーで示している．Alice は**誰でも**彼女にメールが出せるようなメールボックスを用意して，メールがそのメールボックスに入るが，彼女だけがメールを取り出せるようにする．こうするのに彼女はメールボックスに**2つの**ドアを付ける．メールボックスの上には錠付きの跳ね蓋を設けて，誰でも跳ね蓋を開けてメールを入れられるが，落とし口は一方通行で中からメールを取り出すことはできない．Alice は跳ね蓋の鍵を誰でも**自由に得られる**ようにして — これが**公開鍵** (public key) である — 完全に**誰からでも**メールを受け取る．メールボックス前面には第2のドアがありここから中のメールが取り出せる．Alice はこのドアの唯一の鍵を持っている — これが**秘密鍵** (secret key) である —．秘密鍵と公開鍵の2つの鍵を含むこの構成により世界中の誰でもプライバシーを保って Alice と通信できる．

公開鍵暗号システムはこれと同じ原理で働く．Alice は公開鍵を用いてメッセージを受けたいとする．彼女は最初に2つの**暗号鍵** (cryptographic key) — 1つが

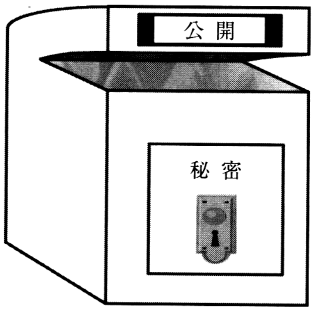



**図 E.1:** 馴染みのある言葉で表現した公開鍵暗号の基本概念．本質的に同じ方法が各国の郵便局で利用されている．

**公開鍵** $P$，もう 1 つが**秘密鍵** $S$ — を作る．これらの鍵の性質はまさに用いる暗号システムの内容に依存している．ある暗号システムでは数のような単純な対象を鍵として用い，別の暗号システムは楕円曲線のようなもっと複雑な数学的対象を鍵として使う．Alice が鍵を作ると，誰でも鍵が得られるように彼女は公開鍵を公表する．

いま Bob が Alice にプライベートなメッセージを送りたいとする．彼は最初に Alice の公開鍵 $P$ をコピーして，この鍵を使って送りたいメッセージを**暗号化** (encrypt) する．実際に暗号変換を行う方法は，用いる暗号システムの詳細に依存する．重要な点は最初にメッセージを暗号化する際に公開鍵を使ったとしても，盗聴に対して安全であるためには，暗号化段階の逆を行うのが非常に難しくなければならない！ これはメールに対する跳ね蓋に似ている — 跳ね蓋の鍵を持っていても一度入れたものは取り出すことはできない．公開鍵と符号化されたメッセージが盗聴者の入手できる唯一の情報なので，盗聴者がメッセージを回復することはできない．しかし Alice は盗聴者が持っていないもう 1 つの情報つまり秘密鍵 $S$ を持っている．この秘密鍵が暗号化したメッセージの第 2 の変換を決定付ける．この変換を**復号化** (decryption) と呼び，暗号化の逆を行って Alice は元のメッセージを回復できる．

これが理想的世界における公開鍵暗号の動作である．本書の執筆時点で公開鍵暗号を達成する安全な方法が存在するかどうかは残念ながらわかっていない．安全であると**広く信じられている**幾つかの方法は確かに存在するが，またインターネット販売のような応用で一般に使われている方法はあるが，広く信じられると

いうことは安全性の証明と等価ではない．これらの方法が安全と信じられる理由はこれらの方法を破る手段を見つけるために非常に多くの努力が払われた（そして不成功に終わった！）からという，一種の摩滅による証明である．この公開鍵暗号のうちで最も広く使われているのが RSA 暗号システムである．RSA の名前は発明者 Rivest, Shamir, Adleman の名前をとっている．推定されている RSA 暗号システムの安全性はこれから調べるように，古典コンピュータ上で素因数分解が明らかに困難であることに基づいている．RSA の理解には整数論の素養が必要であり，この分野は付録 D，特に D.1 節, D.2 節で述べた．

Alice が RSA 暗号システムのための公開鍵と秘密鍵を作りたいとする．彼女は次の手続きを行う：

(1) 2 つの大きな素数 $p$, $q$ を選ぶ．

(2) 積 $n \equiv pq$ を計算する．

(3) $\varphi(n) = (p-1)(q-1)$ と互いに素な小さい奇の整数 $e$ をランダムに選ぶ．

(4) $\varphi(n)$ を法とする $e$ の乗算の逆数 (multiplicative inverse) $d$ を計算する．

(5) **RSA 公開鍵**は対 $P = (e,\ n)$，**RSA 秘密鍵**は対 $S = (d,\ n)$ である．

通信相手の Bob が公開鍵 $P(e,\ n)$ を使って Alice に送るべきメッセージ $M$ を暗号化したいとする．メッセージ $M$ は $\lfloor \log n \rfloor$ ビットだけからなると仮定する．もしこれより長ければ $M$ をたかだか $\lfloor \log n \rfloor$ ビットのブロックに分けて各ブロックを別々に暗号化する．1 つのブロックを暗号化する手続きは次式を計算することである：

$$E(M) = M^e \pmod n. \tag{E.1}$$

$E(M)$ はメッセージ $M$ を暗号化したものであり，これを Bob は Alice に送る．Alice は単に暗号化されたメッセージの $n$ 乗をとることにより彼女の秘密鍵 $S = (d,\ n)$ を使ってただちにメッセージを復号化する：

$$E(M) \to D(E(M)) = E(M)^d \pmod n. \tag{E.2}$$

復号化が成功するには $D(E(M)) = M \pmod n$ である必要がある．これが成り立つには構成上 $ed = 1 \pmod{\varphi(n)}$，つまりある整数 $k$ に対して $ed = 1 + k\varphi(n)$ でなければならない．証明は 2 つの異なる場合に分けて行う．最初の場合は $M$

が $n$ と互いに素な場合である．Euler により一般化された Fermat の小定理 D.9 によれば $M^{k\varphi(n)} = 1 \pmod n$，したがって

$$\begin{aligned} D(E(M)) &= E(M)^d \pmod n &\text{(E.3)}\\ &= M^{ed} \pmod n &\text{(E.4)}\\ &= M^{1+k\varphi(n)} \pmod n &\text{(E.5)}\\ &= M \cdot M^{k\varphi(n)} \pmod n &\text{(E.6)}\\ &= M \pmod n. &\text{(E.7)} \end{aligned}$$

これにより $M$ が $n$ と互いに素のときに復号化は成功することがわかる．次に $M$ は $n$ と互いに素でなく，$p$ と $q$ の一方または両方が $M$ を整除するとする．具体的に $p$ が $M$ を整除する場合を考える．他の場合には少し変形すればよい．$p$ が $M$ を整除するので，$M = 0 \pmod p$，したがって $M^{ed} = 0 = M \pmod p$ である．$q$ は $M$ を整除しないので Fermat の小定理より $M^{q-1} = 1 \pmod q$，したがって $\varphi(n) = (p-1)(q-1)$ なので $M^{\varphi(n)} = 1 \pmod q$ である．$ed = 1 + k\varphi(n)$ を用いると，$M^{ed} = M \pmod q$ である．中国剰余定理から $M^{ed} = M \pmod n$ でなければならず，したがって $M$ が $n$ と互いに素でないときにも復号化は成功する．

**演習 E.1:**　RSA への応用例を書いただけでは不明瞭である．実例で自分自身確かめるのがよい．言葉「QUANTUM」を（あるいは最初の二三の文字だけでも！）一度に 1 文字ずつ $p = 3$, $q = 11$ を用いて暗号化せよ．$e$, $d$ に適切な値を選んで 1 文字当たり 5 ビットを含む英文表現を用いよ．

RSA は如何に効率的に実行できるか？ 実行には考えるべき問題が 2 つある．第 1 は暗号システムのための公開鍵と秘密鍵の作成法である．もしこれが早くできなければ RSA はあまり役に立たない．主な問題点は素数 $p$, $q$ の生成である．これを攻撃する方法は，希望する長さの数をランダムに選んで**素数**テストを行って，この数が実際に素数であることを決める．Miller-Rabin テストのような高速素数テストを使うと，ほぼ $O(L^3)$ 回の演算で数が素数であるかどうかが決められる．ここで $L$ は希望する暗号鍵のサイズである．もしその数が合成数であることがわかれば素数が見つかるまでその手続きを繰り返すだけである．素数定理（問題 D.1）によれば任意の与えられた数が素数である確率は約 $1/\log(2^L) = 1/L$ で

あり，$O(L)$ 回の試行により高確率で素数が得られ鍵生成の全コストは $O(L^4)$ となる．

RSA 実現の第 2 の問題点は暗号化・復号化変換の効率である．これを行うのが剰余指数化 (modular exponentiation) であり，$O(L^3)$ 回の演算で効率良く行えることがわかっている（コラム 5.2 参照）．したがって，RSA 暗号システムを用いるに必要な全演算は古典コンピュータで高速に実行できて，実際に中程度のコンピュータ能力で簡単に数千ビット長までの鍵が処理できる．

RSA を破るにはどうするか？ RSA を破れるかも知れない方法を 2 つ述べる．1 つは位数発見に基づく方法であり，もう 1 つは素因数分解による方法である．Eve が暗号化されたメッセージ $M^e \pmod n$ を受け取り，そのメッセージの暗号化に用いた公開鍵を知っているとする．彼女が暗号化メッセージの位数を見つけられる，つまり $(M^e)^r = 1 \pmod n$ なる最小の正の整数 $r$ を見つけられるとする．（一般性を失うことなくそのような位数が存在する，つまり $M^e$ が $n$ と互いに素であると仮定してよい．もしそうでなければ，$M^e \pmod n$ と $n$ は Euclid のアルゴリズムで求められる公約数を持ち，次の第 2 の方法で述べるようにこれを使って RSA を破ることができる．） このとき演習 D.16 より $r$ は $\varphi$ を整除する．$e$ は $\varphi(n)$ と互いに素なので，$r$ とも互いに素でなければならず，したがって $r$ を法とする乗算の逆数を持つ．$d'$ をその乗算の逆数であるとすると，ある整数 $k$ に対して $ed' = 1 + kr$ である．このとき Eve は暗号化されたメッセージの $d'$ 乗をとることによって元のメッセージ $M$ を得ることができる：

$$
\begin{aligned}
(M^e)^{d'} \pmod n &= M^{1+kr} \pmod n && \text{(E.8)} \\
&= M \cdot M^{kr} \pmod n && \text{(E.9)} \\
&= M \pmod n. && \text{(E.10)}
\end{aligned}
$$

Eve は実際に秘密鍵 $(d,\ n)$ を知らずに $(d',\ n)$ を知るだけでよいのは興味がある．$d'$ は $r$ を法とする $e$ の逆数であり $d$ は $\varphi(n)$ を法とする $e$ の逆数であって $r$ は $\varphi(n)$ を整除するので，もちろん $d'$ は $d$ と密接に関係している．それにもかかわらずこの例は必ずしも秘密鍵の正確な値を決めなくても，RSA が破れることを示している．もちろんこの方法は Eve が位数発見の効率的方法を知っているときにのみ有効であり，現在そのような方法は古典コンピュータ上では知られていない．しかし 5.3.1 節で述べたように，位数発見は量子コンピュータで効率良く実

行できるので RSA を破ることができる．

**演習 E.2:** $d$ も $r$ を法とする $e$ の逆数であり，したがって $d = d' \pmod{r}$ であることを示せ．

RSA を破る第 2 の方法では秘密鍵を完全に決めることができる．Eve は $n = pq$ を素因数分解して $p$, $q$ を取り出し効率的に $\varphi(n) = (p-1)(q-1)$ を計算する手段を持っているとする．Eve にとって $\varphi(n)$ を法とする $e$ の逆数である $d$ を計算することは容易であり，秘密鍵 $(d,\ n)$ を完全に決定できる．もし大きな数の素因数分解が容易ならば RSA を破るのも容易である．

RSA が安全であると思われている根拠は，これらの攻撃が古典コンピュータで処理できないと信じられている（がわかってはいない）問題 — 位数発見と素因数分解問題 — を解くアルゴリズムに依存することにある．不幸にしてたとえこれらの問題が困難であっても，RSA が安全であることは**知られて**さえいない．問題は実際困難であるが RSA を破る方法が何か他にもある可能性もある．これらの警告にもかかわらず 20 年にも及ぶ RSA を破る試みは失敗に帰しており，RSA は古典コンピュータによる攻撃に対して安全であると広く信じられている．

**問題 E.1:** RSA 暗号を用いて暗号化と復号化を行うコンピュータプログラムを書け．20 ビットの素数の一対を求め，それを使って 40 ビットのメッセージを暗号化せよ．

## 歴史と参考資料

公開鍵暗号システムは 1976 年に Diffie と Hellman[DH76] と，ほぼ同時期に独立に Merkle によって発明されたが，Merkle の仕事は 1978 年まで発表されなかった [Mer78]．RSA 暗号システムはその直後に Rivest, Shamir, Adleman によって発明された．1997 年にこれらのアイディア — 公開鍵暗号と Diffie-Hellman および RSA 暗号システム — は実際には英国情報局 GCHQ で働く研究者によって，1960 年代と 1970 年代初めに発明されていたことが公表された．その根拠は http://www.cesg.gov.uk/about/nsecret/ で見られる．Miller-Rabin テストや Solovay-Strassen テストのような素数テストは，整数論と暗号に関する Koblitz

の優れた書 [Kob94] に述べられており，そこには公開鍵暗号のその他の材料が豊富に収録されている．この 2 つの素数テストは，確率的アルゴリズムがある種の目的には決定性アルゴリズムより効率が良いことを示す初期の実例である．Solovay-Strassen のアルゴリズムは Solovay, Strassen [SS76]，Miller-Rabin テストは Miller [Mil76] と Rabin [Rab80] による．

# 参考文献

[注 1] ここには第 II 部（第 II 巻）に関連する参考文献を示す．全体の参考文献は第 I 巻巻末を参照されたい．

[注 2] *arXive e-print quant-ph/xxxxxxx* の文献は http://www.arXiv.org のインターネットサイトから入手できる．


[ADH97] L. Adleman, J. Demarrais, and M. A. Huang. Quantum computability. *SIAM J. Comp.*, 26(5): 1524-1540, 1997.

[AE75] L. Allen and J. H. Eberly. *Optical Resonance and Two-level Atoms*. Dover, New York, 1975.

[Aha99b] D. Aharonov. Quantum computation. In D. Stauffer, editor, *Annual Reviews of Computational Physics VI*. World Scientific, Singapore, 1999.

[AL97] D. S. Abrams and S. Lloyd. Simulation of many-body Fermi systems on a quantum computer. *Phys. Rev. Lett.*, 79(13): 2586-2589, 1997. *arXive e-print quant-ph/9703054*.

[Amb00] A. Ambainis. Quantum lower bounds by quantum arguments. *arXive e-print quant-ph/0002066*, 2000.

[BBBV97] C. H. Bennett, E. Bernstein, G. Brassard, and U. Vazirani. Strengths and weaknesses of quantum computing. *SIAM J. Comput.*, 26(5): 1510-1523, 1997. *arXive e-print quant-ph/9701001* .

[BBC+95] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. Smolin, and H. Weinfurter. Elementary gates for quantum computation. *Phys. Rev. A*, 52: 3457-3467, 1995. *arXive e-print quant-ph/9503016*.

[BBC+98] R. Beals, H. Buhrman, R. Cleve, M. Mosca, and R. de Wolf. Quantum lower bounds by polynomials. In *Proceedings of the 39th Annual Symposium on Foundations of Computer Science (FOCS'98)* , pages 352-361, IEEE, Los Alamitos, California, November 1998. *arXive e-print quant-ph/9802049*.

[BBHT98] M. Boyer, G. Brassard. P. Høyer, and A. Tapp. Tight bounds on quantum searching. *Fortsch. Phys. - Prog. Phys.*, 46(4-5): 493-505, 1998.

[BCDP96] D. Beckman, A. N. Chari, S. Devabhaktuni, and J. Preskill. Efficient networks for quantum factoring. *Phys. Rev. A*, 54(2): 1034, 1996. *arXive e-print quant-ph/9602016*.

[BCJ+99] S. L. Braunstein, C. M. Caves, R. Jozsa, N. Linden, S. Popescu, and R. Schack. Separability of very noisy mixed states and implications for NMR quantum computing. *Phys. Rev. Lett.*, 83(5): 1054-1057, 1999.

[BCJD99] G. K. Brennen, C. M. Caves, P. S. Jessen, and I. H. Deutsch. Quantum logic gates in optical lattices. *Phys. Rev. Lett.*, 82: 1060-1063, 1999.

[BDK92] R. G. Brewer, R. G. DeVoe, and R. Kallenbach. Planar ion microtraps. *Phys. Rev. A*, 46(11): R6781-4, 1992

[Ben80] P. Benioff. The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines. *J. Stat. Phys.*, 22(5): 567-591, 1980.

[Bet84] T. Beth. *Methoden der Schnellen Fouriertransformation.* Teubner, Leipzig, 1984.

[BHT98] G. Brassard, P. Hayer, and A. Tapp. Quantum counting. *arXive e-print quant-ph/9805082,* 1998.

[BK98a] S. L. Braunstein and H. J. Kimble. Teleportion of continuous quantum variables. *Phys. Rev. Lett.,* 80: 869-72, 1998.

[BK99] S. L. Braunstein and H. J. Kimble. Dense coding for continuous variables. *arXive e-print quant-ph/9910010,* 1999.

[BL95] D. Boneh and R. J. Lipton. Quantum cryptoanalysis of hidden linear functions (extended abstract). In Don Coppersmith, editor, *Lecture notes in computer science — Advances in Cryptology — CRYPTO'95*, pages 424-437, Springer-Verlag, Berlin, 1995.

[BMP+99] P. O. Boykin, T. Mor, M. Pulver, V. Roychowdhury, and F. Vatan. On universal and fault-tolerant quantum computing. *arXive e-print quant-ph/9906054,* 1999.

[Bra98] S. L. Braunstein. Error correction for continuous quantum variables. *Phys. Rev. Lett.,* 80: 4084-4087, 1998. *arXive e-print quant-ph/9711049.*

[BT97] B. M. Boghosian and W. Taylor. Simulating quantum mechanics on a quantum computer. *arXive e-print quant-ph/9701019,* 1997.

[BV97] E. Bernstein and U. Vazirani. Quantum complexity theory. *SIAM J. Comput.,* 26(5): 1411-1473, 1997. *arXive e-print quant-ph/9701001* .

[CAK98] N. J. Cerf, C. Adami, and P. Kwiat. Optical simulation of quantum logic. *Phys. Rev. A,* 57: R1477, 1998.

[CEMM98] R. Cleve, A. Ekert, C. Macchiavello and M. Mosca. Quantum algorithms revisited. *Proc. R. Soc. London A,* 454(1969): 339-354, 1998.

[CFH97] D . G. Cory, A. F . Fahmy, and T. F . Havel. Ensemble quantum computing by NMR spectroscopy. *Proc. Nat. Acad. Sci. USA,* 94: 1631-1639, 1997.

[CGK98] I. L. Chuang, N. Gershenfeld and M. Kubinec. Experimental implementation of fast quantum searching. *hys. Rev. Lett.,* 18(15): 3408-3411, 1998.

[CGKL98] I. L. Chuang, N. Gershenfeld, M. G. Kubinec, and D. W. Leung. Bulk quantum computation with nuclear-magnetic-resonance: theory and experiment. *Proc. R. Soc. London A*, 454(1969): 447-467, 1998.

[Che68] P. R. Chernoff. Note on product formulas for operator semigroups. *J. Functional Analysis,* 2: 238-242, 1968.

[Cla89] M. Clausen. Fast generalized Fourier transforms. *Theor. Comput. Sci.,* 67: 55-63, 1989.

[Cle99] R. Cleve. The query complexity of order-finding. *arXive e-print quant-ph/9911124,* 1999.

[CLR90] T. H. Cormen, C. E. Leiserson, R. L. Rivest. *Introduction to Algorithms.* MIT Press, Cambridge, Mass., 1990.

[CMP+98] D. G. Cory, W. Mass, M. Price, E. Knill, R. Laflamme, W. H. Zurek, T. F. Havel, and S. S. Somaroo. Experimental quantum error correction. *arXive e-print quant-ph/9802018,* 1998.

[Cop94] D. Coppersmith. An approximate Fourier transform useful in quantum factoring. *IBM Research Report RC 19642*, 1994.

[CST89] R. A. Campos, B. E. A. Saleh, and M. C. Tiech. Quantum-mechanical lossless beam-splitters: SU(2) symmetry and photon statistics. *Phys. Rev. A,* 40: 1371, 1989.

[CVZ+98] I. L. Chuang, L. M. K. Vandersypen, X. L. Zhou, D. W. Leung, and S. Lloyd. Experimental realization of a quantum algorithm. *Nature,* 393(6681): 143-146, 1998.

[CW95] H. F. Chau and F. Wilczek. Simple realization of the Fredkin gate using a series of two-body operators. *Phys. Rev. Lett.,* 75(4): 748-50, 1995. *arXive e-print quant-ph/9503005.*

[CY95] I. L. Chuang and Y. Yamamoto. Simple quantum computer. *Phys. Rev. A,* 52: 3489-3496, 1995. *arXive e-print quant-ph/9505011.*

[CZ95] J. I. Cirac and P. Zoller. Quantum computations with cold trapped ions. *Phys. Rev. Lett.,* 74: 4091, 1995.

[DBE95] D. Deutsch, A. Barenco, and A. Ekert. Universality in quantum computation. *Proc. R. Soc. London A,* 449(1937): 669-677, 1995.

[Deu85] D. Deutsch. Quantum theory, the Church-Turing Principle and the universal quantum computer. *Proc. R. Soc. Lond. A, 400: 97, 1985.*

[Deu89] D. Deutsch. Quantum computational networks. *Proc. R. Soc. London A,* 425: 73, 1989.

[DH76] W. Diffie and M. Hellman. New directions in cryptography. *IEEE Trans. Inf. Theory,* IT-22(6): 644-54, 1976.

[DH96] C. Dürr and P. Høyer. A quantum algorithm for finding the minimum. *arXive e-print quant-ph/9607014,* 1996.

[DiV95a] D. P. DiVincenzo. Quantum computation. *Science,* 270: 255, 1995.

[DiV95b] D. P. DiVincenzo. Two-bit gates are universal for quantum computation. *Phys. Rev. A,* 51(2): 1015-1022, 1995.

[DiV98] D. P. DiVincenzo. Quantum gates and circuits. *Proc. R. Soc. London A,* 454: 261-276, 1998.

[DMB+93] L. Davidovich, A. Maali, M. Brune, J. M. Raimond, and S. Haroche. *Phys. Rev. Lett.,* 71: 2360, 1993.

[DR90] P. Diaconis and D. Rockmore. Efficient computation of the Fourier transform on finite groups. *J. Amer. Math. Soc.,* 3(2): 297-332, 1990.

[DRBH87] L. Davidovich, J. M. Raimond, M. Brune, and S. Haroche. *Phys. Rev. A,* 36: 3771, 1987.

[DRBH95] P. Domokos, J. M. Raimond, M. Brune, and S. Haroche. Simple cavity-QED two-bit universal quantum logic gate: The principle and expected performances. *Phys. Rev. Lett.,* 52: 3554, 1995.

[Ear42] S. Earnshaw. On the nature of the molecular forces which regulate the constitution of the luminiferous ether. *Trans. Camb. Phil. Soc.,* 7: 97-112, 1842.

[EBW87] R. R. Ernst, G. Bodenhausen, and A. Wokaun. *Principles of Nuclear Magnetic Resonance in One and Two Dimensions.* Oxford University Press, Oxford, 1987.

[EH99] M. Ettinger and P. Høyer. On quantum algorithms for noncommutative hidden subgroups. In *Symposium on Theoretical Aspects in Computer Science.* Universitv of Trier, 1999. *arXive e-print quant-ph/9807029.*

[EHK99] M. Ettinger, P. Høyer, and E. Knill. Hidden subgroup states are almost orthogonal. *arXive e-print quant-ph/9901034,* 1999.

[EJ96] A. Ekert and R. Jozsa. Quantum computation and Shor's factoring algorithm. Rev. Mod. Phys., 68: 733, 1996.

[EJ98] A. Ekert and R. Jozsa. Quantum algorithm: Entanglement enhanced information prosessing. *Proc. R. Soc. London A,* 356(1743): 1769-82, Aug. 1998. *arXive e-print quant-ph/803072.*

[Fey82] R. P. Feynman. Simulating physics computers. *Int. J. Theor. Phys.,* 21: 467, 1982.

[FG98] E. Farhi and S. Gutmann. An analog analogue of a digital quantum computation. Phys. Rev. A, 57(4): 2403-2406, 1998. *arXive e-print quant-ph/9612026.*

[FS92] A. Fässler and E. Stiefel. *Group Theoretical Methods and Their Applications.* Birhaüser, Boston, 1992.

[FSB+98] A. Furusawa, J. L. Sørensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble, and E. S. Polzik. Unconditional quantum teleportation. *Science,* 282: 706-709, 1998.

[Gar91] C. W. Gardiner. *Quantum Noise.* Springer-Verlag, Berlin, 1991.

[GC97] N. Gershenfeld and I. L. Chuang. Bulk spin resonance quantum computation. *Science,* 275: 350, 1997.

[GC99] D. Gottesman and I. L. Chuang. Quantum teleportation is a universal computational primitive. *Nature,* 402: 390-392, 1999. *arXive e-print quant-ph/9908010.*

[GN96] R. B. Griffiths and C.-S. Niu. Semiclassical Fourier transform for quantum computation. *Phys. Rev. Lett.,* 76(17): 3228-3231, 1996. arXive e-print quant-ph/9511007.

[Gro96] L. Grover. In *Proc. 28th Annual ACM Symposium on the Theory of Computation,* pages 212-219, ACM Press, New York, 1996

[Gro97] L. K. Grover. Quantum mechanics helps in searching for a needle in a haystack. *Phys. Rev. Lett.,* 79(2): 325, 1997. *arXive e-print quant-ph/9706033.*

[Ham89] M. Hammermesh. *Group Theory and its Application to Physical Problems.* Dover, New York, 1989.

[HSM+98] A. G. Huibers, M. Switkes, C. M. Marcus, K. Campman, and A. C. Gossard. Dephasing in open quantum dots. *Phys. Rev. Lett.,* 82: 200, 1998.

[HW60] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers. Fourth Edition.* Oxford University Press, London, 1960.

[IAB+99] A. Imamoglu, D. D. Awschalom, G. Burkard, D. P. DiVincenzo, D. Loss, M. Sherwin, and A. Small. Quantum information processing using quantum dot spins and cavity QED. *Phys. Rev. Lett.,* 83(20): 4204-7, 1999.

[IY94] A. Imamoglu and Y. Tamamoto. Turnstile device for heralded single photons: Coulomb blockade of electron and hole tunneling in quantum confined p-i-n heterojunctions. *Phys. Rev. Lett.,* 72(2): 210-13, 1994.

[Jam98] D. James. The theory of heating of the quantum ground state of trapped ions. *arXive e-print quant-ph/9804048,* 1998.

[Jay57] E. T. Jaynes. Information theory and statistical mechanics. ii. *Phys. Rev.,* 108(2): 171-190, 1957.

[JM98] J. A. Jones and M. Mosca. Implementation of a quantum algorithm to solve Deutsch's problem on a nuclear magnetic resonance quantum computer. *arXive e-print quant-ph/9801027,* 1998.

[JMH98] J. A. Jones, M. Mosca, and R. H. Hansen. Implementation of a quantum search algorithm on a nuclear magnetic resonance quantum computer. *Nature,* 393(6683): 344, 1998. *arXive e-print quant-ph/9805069.*

[Joz97] R. Jozsa. Quantum algorithms and the Fourier transform. *arXive e-print quant-ph/9707033,* 1997.

[Kan98] B. Kane. A silicon-based nuclear spin quantum computer. *Nature,* 393: 133-137, 1998.

[KCL98] E. Knill, I. Chuang, and R. Laflamme. Effective pure states for bulk quantum computaion. *Phys. Rev. A,* 57(5): 3348-3363, 1998. *arXive e-print quant-ph/9706053.*

[Kit95] A. Y. Kitaev. Quantum measurements and the Abelian stabilizer problem. *arXive e-print quant-ph/9511026,* 1995.

[Kit97b] A. Y. Kitaev. Quantum computations: algorithm and error correction. *Russ. Math. Surv.,* 52(6): 1191-1249, 1997.

[KL99] E. Knill and R. Laflamme. Quantum computation and quadratically signed weight enumerators. *arXive e-print quant-ph/9909094,* 1999.

[KMSW99] P. G. Kwiat, J. R. Mitchell, P. D. D. Schwindt, and A. G. White. Grover's search algorithm: An optical approach. *arXive e-print quant-ph/9905086,* 1999.

[Kni95] E. Knill. Approximating quantum circuits. *arXive e-print quant-ph/9508006,* 1995.

[Kob94] N. Koblitz. *A Course in Number Theory aand Cryptography.* Springer-Verlag, New York, 1994.

[KSC+94] P. G. Kwiat, A. M. Steinberg, R. Y. Chiao, P. H. Eberhard, and M. D. Petroff. Absolute efficiency and time-response measurement of single-photon detectors. *Appl. Opt.,* 33(10): 1844-1853, 1994.

[KU91] M. Kitagawa and M. Ueda. Nonlinear-interferometric generation of number-phase correlated Fermion states. *Phys. Rev. Lett.,* 67(14): 1852, 1991.

[LB99] S. Lloyd and S. Braunstein. Quantum computation over continuous variables. *Phys. Rev. Lett.,* 82: 1784-1787, 1999. *arXive e-print quant-ph/9810082.*

[LD98] D. Loss and D. P. DiVincenzo. Quantum computation with quantum dots. *Phys. Rev. A,* 57: 120-126, 1998.

[LKF99] N. Linden, E. Kupce, and R. Freeman. NMR quantum logic gates for homonuclear spin systems. *arXive e-print quant-ph/9907003,* 1999.

[LL93] A. K. Lenstra and H. W. Lenstra Jr., editors. *The Development of the Number Field Sieve.* Springer-Verlag, New York, 1993.

[Llo93] S. Lloyd. A potentially realizable quantum computer. *Science,* 261: 1569, 1993.

[Llo94] S. Lloyd. Necessary and sufficient conditions for quantum computation. *J. Mod. Opt.,* 41(12): 2503, 1994.

[Llo95] S. Lloyd. Almost any quantum logic gate is universal. *Phys. Rev. Lett.,* 75(2): 346, 1995.

[Lom87] J. S. Lomont. *Applications of Finite Groups.* Dover, New York, 1987.

[Lou73] W. H. Louisell. *Quantum Statistical Properties of Radiation.* Wiley, New York, 1973.

[LP99] N. Linden and S. Popescu. Good dynamics versus bad kinematics. Is entanglement needed for quantum computation? *arXive e-print quant-ph/9906008,* 1999.

[LS98] S. Lloyd and J. E. Slotine. Analog quantum error correction. *Phys. Rev. Lett.,* 80: 4088-4091, 1998.

[LVZ+99] D. W. Leung, L. M. K. Vandersypen, X. Zhou, M. Sherwood, C. Yannoni, M. Kubinec, and I. L. Chuang. Experimental realization of a two-bit phase damping quantum code. *Phys. Rev. A,* 60: 1924, 1999.

[Man80] Y. Manin. *Computable and Uncomputable (in Russian)* . Sovetskoye Radio, Moscow, 1980.

[Man99] Y. I. Manin. Classical computing, quantum computing, and Shor's factoring algorithm. *arXive e-print quant-ph/9903008,* 1999.

[ME99] M. Mosca and A. Ekert. The hidden sub-group problem and eigenvalue estimation on a quantum computer. *arXive e-print quant-ph/9903071,* 1999.

[Mer78] R. Merkle. Secure communications over insecure channels. *Comm. of the ACM,* 21: 294-299, 1978.

[Mil76] G. L. Miller. Riemann's hypothesis and tests for primality. *J. Comput. Syst. Sci.,* 13(3): 300-317, 1976.

[Mil89a] G. J. Milburn. Quantum optical Fredkin gate. *Phys. Rev. Lett.,* 62(18): 2124, 1989.

[Mil89b] D. A. B. Miller. Optics for low energy communications inside digital processors: quantum detectors, sources, and modulators as efficient impedance converters. *Opt. Lett.,* 14: 146, 1989.

[MMK+95] C. Monroe, D. M. Meekhof, B. E. King, W. M. Itano, and D. J. Wineland. Demonstration of a fundamental quantum logic gate. *Phys. Rev. Lett.,* 75: 4714, 1995.

[MOL+99] J. E. Mooij, T. P. Orlando, L. Levitov, L. Tian, C. H. van der Waal, and S. Lloyd. Josephson persistent-current qubit. *Science,* 285: 1036-1039, 1999.

[Mos98] M. Mosca. Quantum searching, counting and amplitude amplification by eigenvector analysis. In R. Freivalds, editor, *Proceedings of International Workshop on Randomized Algorithms,* pages 90-100, 1998.

[Mos99] M. Mosca. *Quantum Computer Algorithms.* Ph.D. thesis, University of Oxford, 1999.

[NKL98] M. A. Nielsen, E. Knill, and R. Laflamme. Complete quantum teleportation using nuclear magnetic resonance. *Nature,* 396(6706): 52-55, 1998.

[NPT99] Y. Nakamura, Y. A. Pashkin, and J. S. Tsai. Coherent control of macroscopic quantum states in a single-cooper-pair box. *Nature,* 398: 786-788, 1999.

[Pap94] C. M. Papadimitriou. *Computational Complexity.* Addison-Wesley, Reading, Massachusetts, 1994.

[PD99] P. M. Platzman, and M. I. Dykman. Quantum computing with electrons floating on liquid helium. *Science,* 284: 1967, 1999.

[PK96] M. B. Plenio and P. L. Knight. Realistic lower bounds for the factorization time of large numbers on a quantum computer. *Phys. Rev. A,* 53: 2986-2990, 1996.

[Pop75] R. P. Poplavskii. Thermodynamical models of information processing (in Russian). *Usp. Fiz. Nauk,* 115(3): 465-501, 1975.

[PRB98] M. Pueschel, M. Roetteler, and T. Beth. Fast quantum Fourier transforms for a class of non-abelian groups. *arXive e-print quant-ph/9807064,* 1998.

[Rab80] M. O. Rabin. Probabilistic algorithm for testing primarity. *J. Number Theory,* 12: 128-138, 1980.

[RB98] M. Roetteler and T. Beth. Polynomial-time solution to the hidden subgroup problem for a class of non-abelian groups. *arXive e-print quant-ph/9812070,* 1998.

[RSA78] R. L. Rivest, A. Shamir, and L. M. Adleman. A method of obtaining digital signatures and public-key cryptosystems. *Comm. ACM,* 21(2): 120-126, 1978.

[RWvD84] S . Ramo , J. R. Whinnery , and T. van Duzer. *Fields and waves in communication electronics.* Wiley, New York, 1984.

[RZBB94] M. Reck, A. Zeilinger, H. J. Bernstein, and P. Bertani. Experimental realization of any discrete unitary operator. *Phys. Rev. Lett.,* 73(1): 58-61, 1994.

[Sak95] J. J. Sakurai. *Modern Quantum Mechanics.* Addison-Wesley, Reading, Mass., 1995.

[SC99] R. Schack and C. M. Caves. Classical model for bulk-ensemble NMR quantum computation. *Phys. Rev. A,* 60(6): 4354-4362, 1999.

[Sho94] P. W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings, 35th Annual Symposium on Foundations of Computer Science,* IEEE Press, Los Alamitos, CA, 1994.

[Sho97] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comp.,* 26(5): 1484-1509, 1997.

[Sim94] D. Simon. On the power of quantum computation. In *Proceedings. 35th Annual Symposium on Foundations of Computer Science,* pages 116-123, IEEE Press, Los Alamitos, CA, 1994.

[Sim97] D. R. Simon. On the power of quantum computation. *SIAM J. Comput.,* 26(5): 1474-1483, 1997.

[Sli96] C. P. Slichter. *Principles of Magnetic Resonance.* Springer, Berlin, 1996.

[SS76] R. Solovay and V. Strassen. A fast Monte-Carlo test for primality. *SIAM J. Comput.,* 6: 84-85, 1976.

[SS99] A. T. Sornborger and E. D. Stewart. Higher order methods for simulations on quantum computers. *Phys. Rev. A,* 60(3): 1956-1965, 1999. *arXive e-print quant-ph/9903055.*

[ST91] B. E. A. Saleh and M. C. Teich. *Fundamentals of Photonics.* Wiley, NY, 1991.

[Ste97] A. Steane. The ion-trap quantum information processor. *Appl . Phys. B - Lasers and Optics,* 64(6): 623-642, 1997.

[STH+99] S. Somaroo, C. H. Tseng, T. F. Havel, R. Laflamme, and D. G. Cory. Quantum simulations on a quantum computer. *Phys. Rev. Lett.,* 82: 5381-5384, 1999.

[SV99] L. J. Schulman and U. Vazirani. Molecular scale heat engines and scalable quantum computation. *Proc. 31st Ann. ACM Symp. on Theory of Computing (STOC '99)*, pages 322-329, 1999.

[TD98] B. M. Terhal and D. P. DiVincenzo. The problem of equilibration and the computation of correlation functions on a quantum computer. *arXive e-print quant-ph/9810063*, 1998.

[THL+95] Q. A. Turchette, C. J. Hood, W. Lange, H. Mabuchi, and H. J. Kimble. Measurement of conditional phase shifts for quantum logic. *Phys. Rev. Lett.*, 75: 4710, 1995.

[Tro59] H. F. Trotter. On the product of semigroups of operators. *Proc. Am. Math. Soc.*, 10: 545-551, 1959.

[Tur97] Q. A. Turchette. *Quantum optics with single atoms and single photons*. Ph.D. thesis, California Institute of Technology, Pasadena, California, 1997.

[Vai94] L. Vaidman. Teleportation of quantum states. *Phys. Rev. A*, 49(2): 1473-6, 1994.

[van98a] W. van Dam. Quantum oracle interrogation: getting all information for half the price. In *Proceedings of the 39th FOCS*, 1998. *arXive e-print quant-ph/9805006*.

[Vid99] G. Vidal. Entanglement of pure states for a single copy. *Phys. Rev. Lett.*, 83(5): 1046-1049, 1999.

[VYSC99] L. M. K. Vandersypen, C. S. Yannoni, M. H. Sherwood, and I. L. Chuang. Realization of effective pure states for bulk quantum computation. *Phys. Rev. Lett.*, 83: 3085-3088, 1999.

[VYW+99] R. Vrijen, E. Yablonovitch, K. Wang, H. W. Jiang, A. Balandin, V. Roychowdhury, T. Mor, and D. DiVincenzo. Electron spin resonance transistors for quantum computing in silicon-germanium heterostructures. *arXive e-print quant-ph/9905096*, 1999

[War97] W. Warren. The usefulness of NMR quantum computing. *Science*, 277(5332): 1688, 1997.

[Wat99] J. Watrous. **PSPACE** has 2-round quantum interactive proof systems. *arXive e-print cs/9901015*, 1999.

[Wie96] S. Wiesner. Simulations of many-body quantum systems by a quantum computer. *arXive e-print quant-ph/9603028*, 1996.

[WMI+98] D. J. Wineland, C. Monroe, W. M. Itano, D. Leibfried, B. E. King, and D. M. Meekhof. Experimental issues in coherent quantum-state manipulation of trapped atomic ions. *J. Res. Natl. Inst. Stand. Tech.*, 103: 259, 1998.

[WY90] K. Watanabe and Y. Yamamoto. Limits on tradeoffs between third-order optical nonlinearity, absorption loss, and pulse duration in self-induced transparency and real excitation. *Phys. Rev. A*, 42(3): 1699-702, 1990.

[Yao93] A. C. Yao. Quantum circuit complexity. *Proc. of the 34th Ann. IEEE Symp. on Foundations of Computer Science*, pages 352-361, 1993.

[YKI88] Y. Yamamoto. M. Kitagawa, and K. Igeta. In *Proc. 3rd. Asia-Pacific Phys. Conf.*, World Scientific, Singapore, 1988.

[YY99] F. Yamaguchi and Y. Yamamoto. Crystal lattice quantum computer. *Appl. Phys. A*, pages 1-8, 1999.

[Zal98] C. Zalka. Simulating quantum systems on a quantum computer. *Proc. R. Soc. London A*, 454(1969): 313-322, 1998.

[Zal99] C. Zalka. Grover's quantum searching algorithm is optimal. *Phys. Rev. A*, 60(4): 2746-2751, 1999.

[ZHSL99] K. Zyczkowski, P. Horodecki, A. Sanpera, and M. Lewenstein. Volume of the set of separable states. *Phys. Rev. A*, 58(2): 883-892, 1999.

# 索　引

〈著者・訳者の紹介〉

Michael A. Nielsen（ミカエル ニールセン）

現在，クイーンズランド大学において量子情報研究財団の教授とオーストラリア研究協議連盟のフェローを務める．出身はオーストラリアのブリスベン．クイーンズランド大学で数学と物理学の大学院を修了した後，米国ニューメキシコ大学においてFulbright奨学生となり物理学の学位を取得．その後，カリフォルニア工科大学でTolmanポストドクター研究員を務め，2000年にオーストラリアに戻り現職．

Isaac L. Chuang（アイザック チャン）

現在マサチューセッツ工科大学（MIT）・物理学部の準教授．同大学メディア研究所のビットと原子研究センターにおいて量子情報科学研究グループを率いる．出身はケンタッキー州ルイズビル．スタンフォード大学においてHertz財団フェローとなり，電気工学の学位を取得．さらにMITから物理学と電気工学の学位も得る．趣味は読書，ハイキングおよびバイオリンの演奏．

木 村 達 也（きむら たつや）

東京大学大学院工学系研究科を修了，工学博士の学位を取得．NTT研究所において光伝送方式，光ファイバ，光部品に関する基礎研究を進め，長波長帯光ファイバ伝送や光増幅中継等の先端的光ファイバ通信を提唱．その後，材料物性および情報科学の基礎研究マネジメントに従事して，量子光学，ナノサイエンス，情報科学の研究を推進し，NTT理事・基礎研究所長，NEC支配人を歴任．現在NTTアドバンステクノロジ(株)シニアアドバイザを務める．IEEEフェロー，IEICEフェロー，OSA名誉会員．



量子コンピュータと量子通信 II ―量子コンピュータとアルゴリズム―

平成17年1月10日　第1版第1刷発行

| | |
|---|---|
| 著　者 | Michael A. Nielsen<br>Isaac L. Chuang |
| 訳　者 | 木 村 達 也 |
| 発行者 | 佐 藤 政 次 |
| 発行所 | 株式会社 オーム社<br>郵便番号 101-8460<br>東京都千代田区神田錦町3-1<br>電 話 03(3233)0641(代表)<br>URL http://www.ohmsha.co.jp/ |



印刷　中央印刷　　製本　三水舎
ISBN4-274-20008-6　Printed in Japan